Enterprise Network Design and Deployment

Project Lead: Haim Levhar
ID Number: 329458632
Instructor: Itzik Zvi
Year of Execution: 2025
School: Sitrin

Table of Contents

ACKNOWLEDGEMENTS

First and foremost, I would like to express my immense gratitude to the *Almighty* for granting me the opportunity, patience, and perseverance throughout the entire execution of the project, both during the learning phase and the implementation phase.

Wendell Odom, whose CCNA series has significantly impacted this project, was priceless to me during this time. I want to thank *Yishai Shobali*, a considerate person who facilitated me and suggested great ideas throughout this development. I would also like to thank *Ariel Levi,* a great individual who helped me solidify my understanding of concepts and strengthen my troubleshooting skills along this journey. Thanks to *Itzik Tzvi* for his suggestions of improvements and revisions that I did not notice along crucial modifications executed to be in accordance with the network requirements, transforming this project to a near-perfection with respective to its requirements. Thanks to classmates who had taken part in this project. Additionally, I would like to acknowledge *Chat GPT* for its valuable assistance in handling the more tedious aspects of this process.

Project Overview

Company Profile: Mentora Nexus

Founders: Yami Sukehiro, Eran Yeager
Industry Sectors: Academic Publishing, E-Learning, Technology
Revenue: $75 million (2024)
CEO: Light Yagami

Mentora Nexus is a leading provider of academic resources focused on computer science, based in Innovation Valley, California, USA. Founded in 2010 by Yami Sukehiro and Eran Yeager, the company began as a specialized library dedicated to programming, software engineering, and related computer science disciplines. Over the years, Mentora Nexus has evolved into a trusted name in digital learning, offering high-quality textbooks, AI-powered study tools, and customized learning resources.

With a focus on empowering students and professionals, Mentora Nexus launched its e-commerce platform in 2015, providing global access to curated academic materials. The organization has introduced AI-driven learning paths and personalized recommendations to enhance the educational experience for users at all levels.

Mentora Nexus specializes in advanced topics such as artificial intelligence, data science, and cybersecurity, aligning with your interest in computer science and philosophy-based approaches to learning. The company also emphasizes sustainable practices, including digital-first solutions and carbon-neutral initiatives.

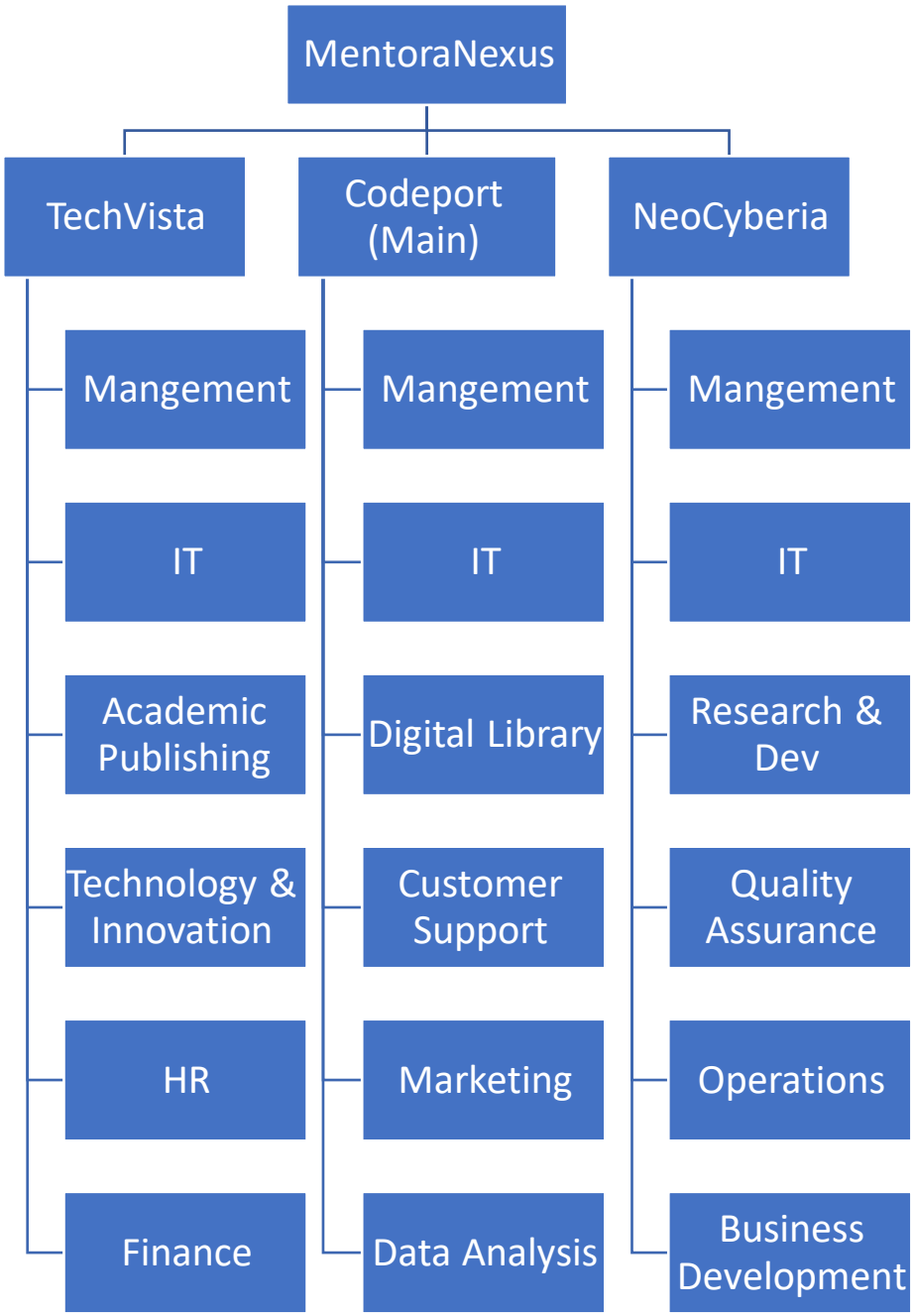
In the coming years, Mentora Nexus aims to expand access to rare academic materials, foster global academic communities, and continue innovating in the field of computer science education.

The main branch, branch 1, and branch 2 are located on **Haifa**, **Tel Aviv**, and **Ashkelon**, respectively.

Network Requirements and Solutions

Network Requirement	Solutions
Manage company emails and enable email exchange between employees.	Set up **POP3** and **SMTP** servers.
Provide internal storage for company files.	Establish **FTP** servers for secure storage and retrieval of internal organizational data.
Enable employee access to client management applications and data through user-friendly domain names instead of IP addresses.	Set up internal **WEB servers** and implement a **DNS server** to translate IP addresses into domain names.
Ensure fast communication between company branches.	Use **Metro Ethernet** infrastructure with fiber-optic connectivity provided by the ISP.
Maintain smooth, fast, and load-free internal network traffic.	Design an optimized network structure, implement **VLANs** for different departments, and divide into subnets.
Allow the network administrator to manage the network remotely.	Enable remote access (**VTY**) to routers and switches.
Provide wireless internet access for employees and visitors.	Implement wireless access points (**WAPs**) for secure connectivity via mobile phones, tablets, and laptops.
Enable selective internet access for certain employees.	Connect to an ISP and implement **ACLs** on the outbound router.

Organizational Chart and Departmental Objectives



Branch Organizational Overview

TechVista Branch

Department Name	Objective	Number of Employees
Management	Oversee and direct overall operations to ensure alignment with the organization's mission, vision, and strategic goals	10
Information Technology (IT)	Manage and develop the technological infrastructure supporting both physical and digital operations, ensuring a seamless user experience	7
Academic Publishing	Curate and publish high-quality academic textbooks, with a focus on emerging fields such as artificial intelligence, data science, and cybersecurity	7
Technology & Innovation	Integrate advanced technologies into services, including AI-driven recommendations and personalized learning resources	7
Human Resource (HR)	Manage recruitment, training, and employee relations to foster a positive and productive work environment	7
Finance	Handle financial planning, budgeting, and resource management to ensure the economic sustainability of the organization	8

Codeport Branch - Main

Department Name	Objective	Number of Employees
Management	Oversee and direct overall operations to ensure alignment with the organization's mission, vision, and strategic goals	11
Information Technology (IT)	Manage and develop the technological infrastructure supporting both physical and digital operations, ensuring a seamless user experience	8
Digital Library	Manage the digital collection of textbooks and resources, making them accessible globally and supporting eco-friendly initiatives	8
Customer Support	Provide assistance and support to users, ensuring a positive customer experience.	8
Marketing	Promote the organization's services and products to expand reach and brand recognition within the academic community.	8
Data Analysis	Analyze data to drive decision-making, improve services, and tailor resources to meet users' needs	9

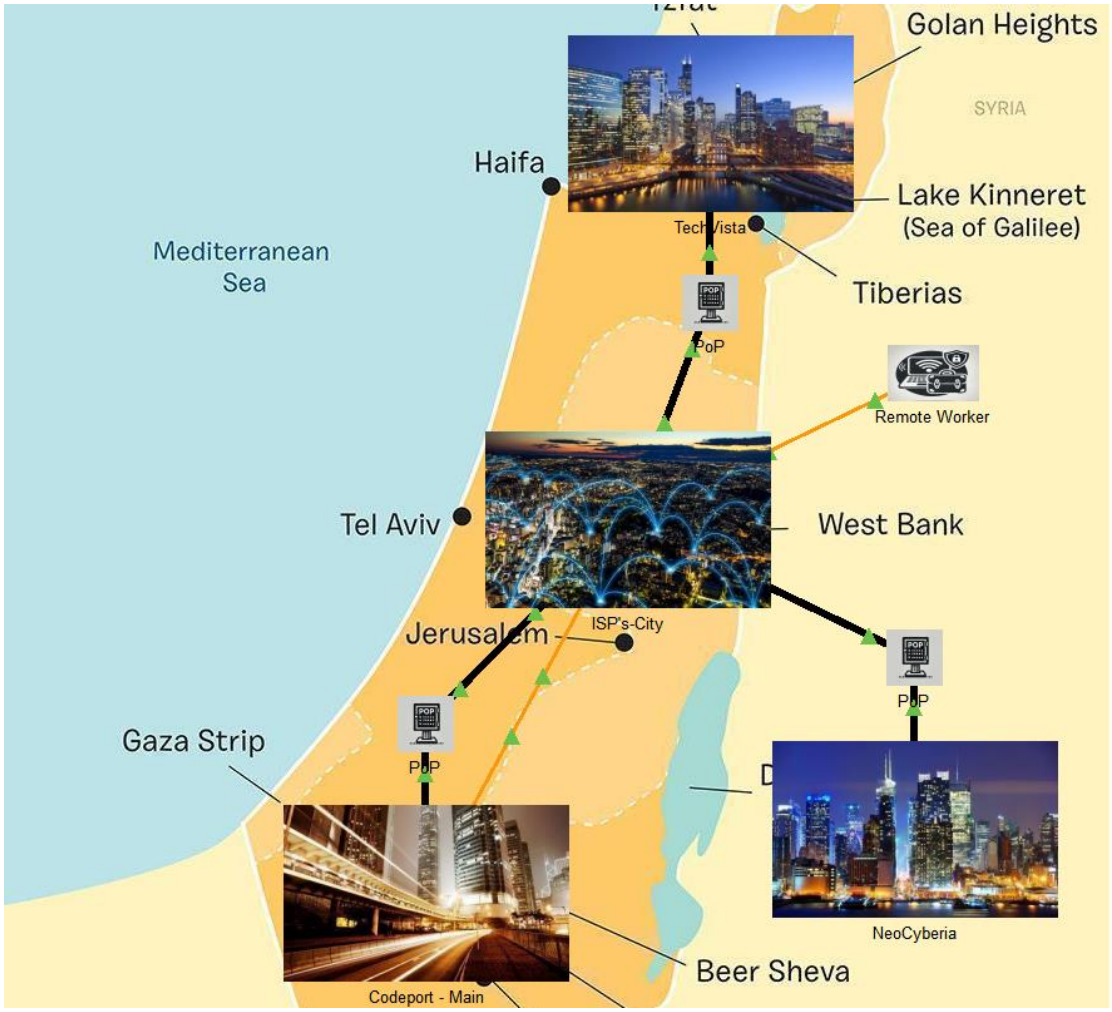
NeoCyberia Branch

Department Name	Objective	Number of Employees
Management	Oversee and direct overall operations to ensure alignment with the organization's mission, vision, and strategic goals	9
Information Technology (IT)	Manage and develop the technological infrastructure supporting both physical and digital operations, ensuring a seamless user experience	6
Research & Development	Innovate and develop new products, services, and technologies to enhance the learning experience.	6
Quality Assurance	Ensure that all products and services meet high standards of quality and reliability	6
Operations	Manage day-to-day activities to ensure efficiency and effectiveness in all aspects of the organization's operations	6
Business Development	Identify new business opportunities, partnerships, and growth strategies.	7

Physical and Logical Topologies view

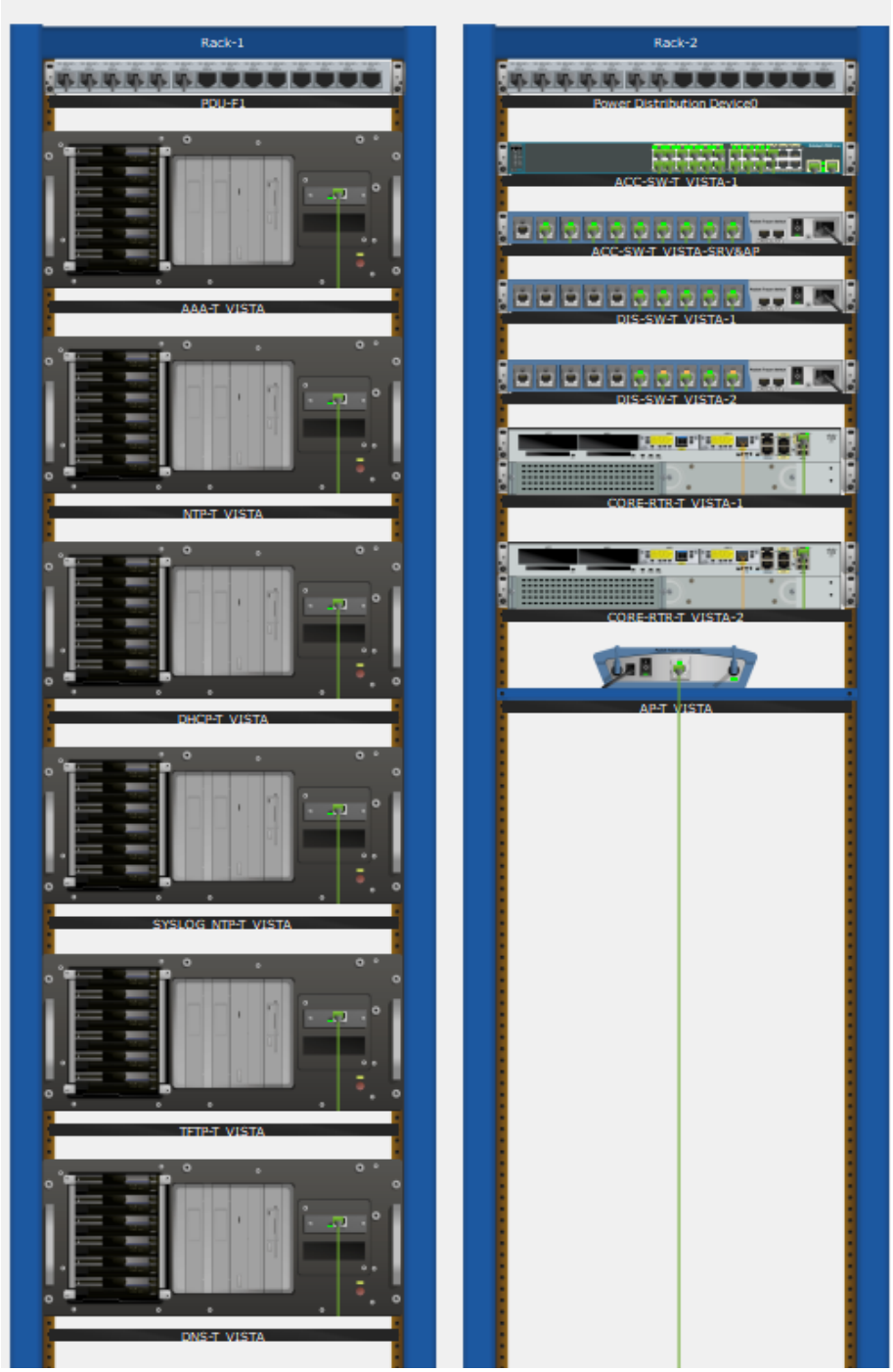
Physical Topology View

Branches Map

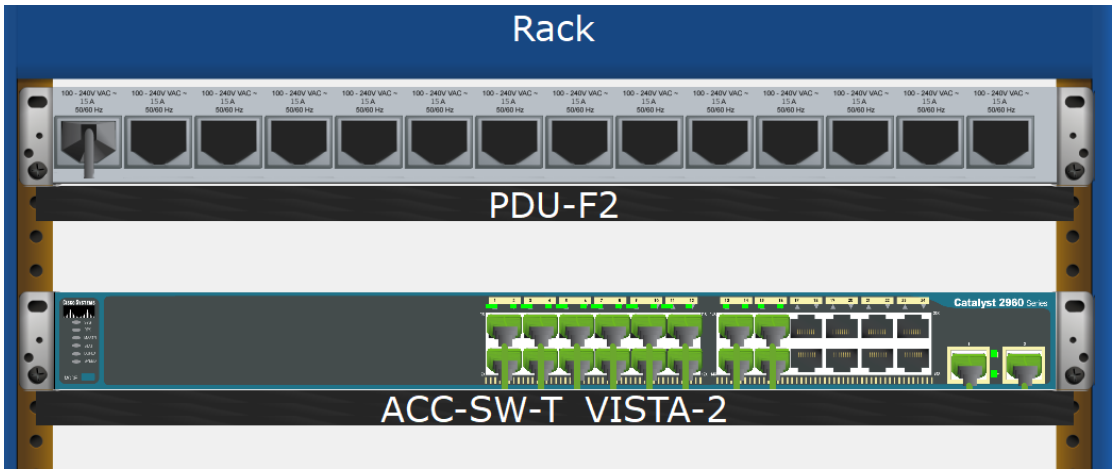


TechVista Branch

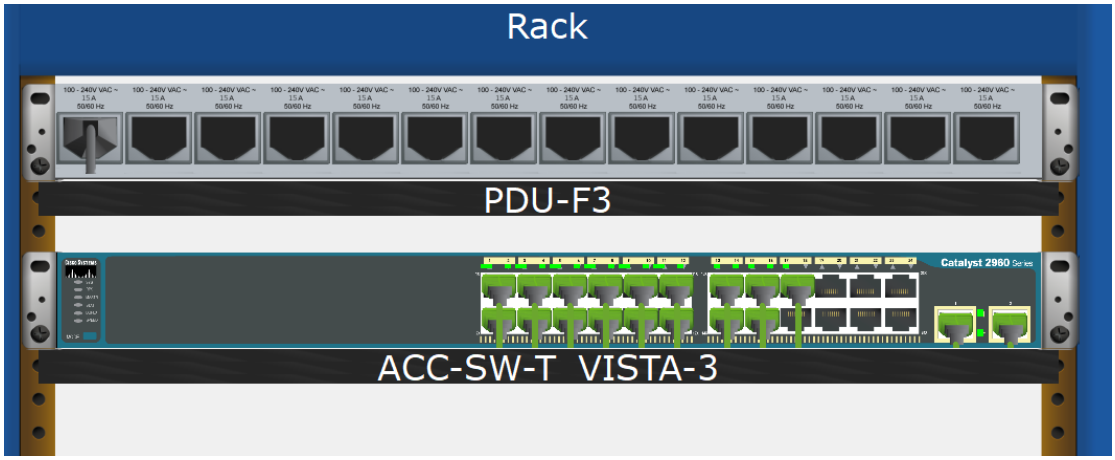
First Floor



Second Floor

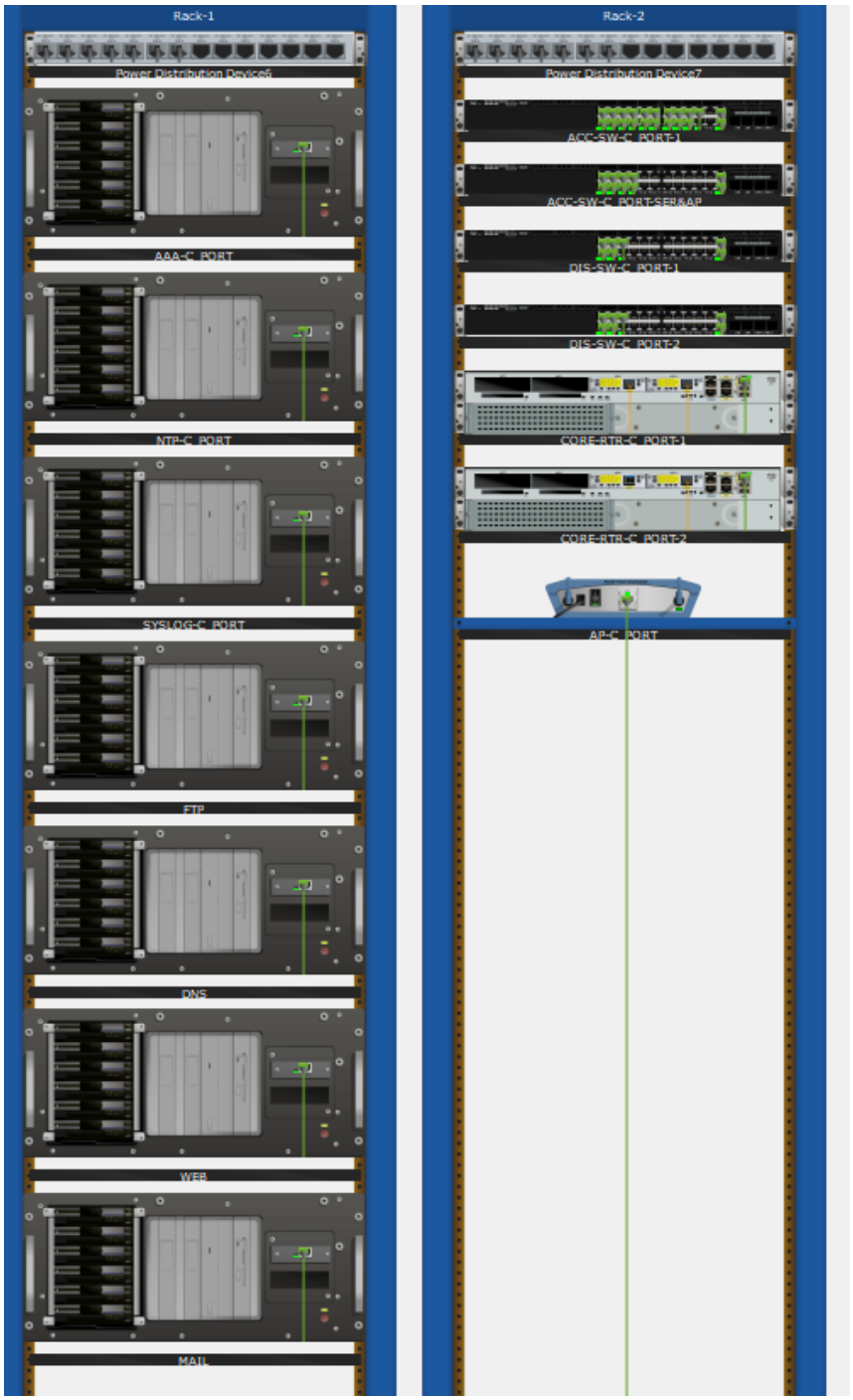


Third Floor

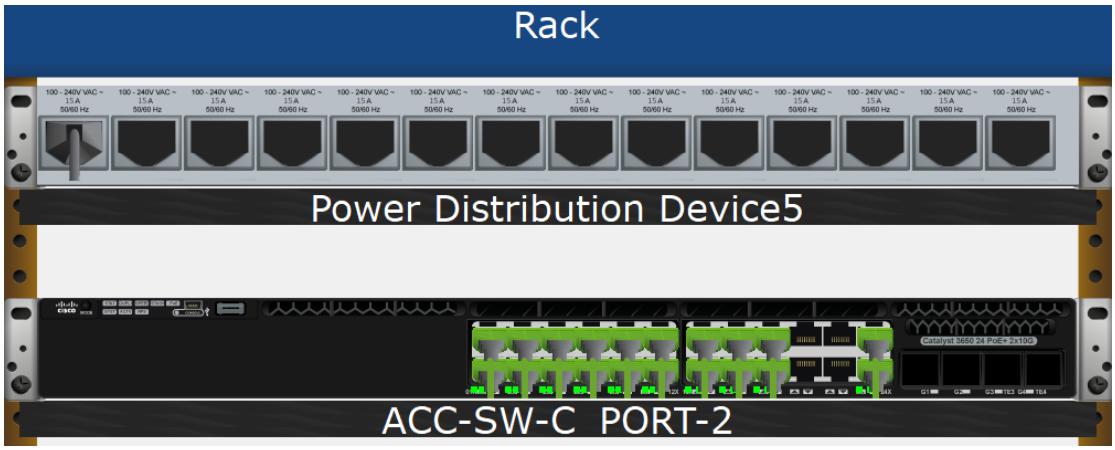


CodePort Branch

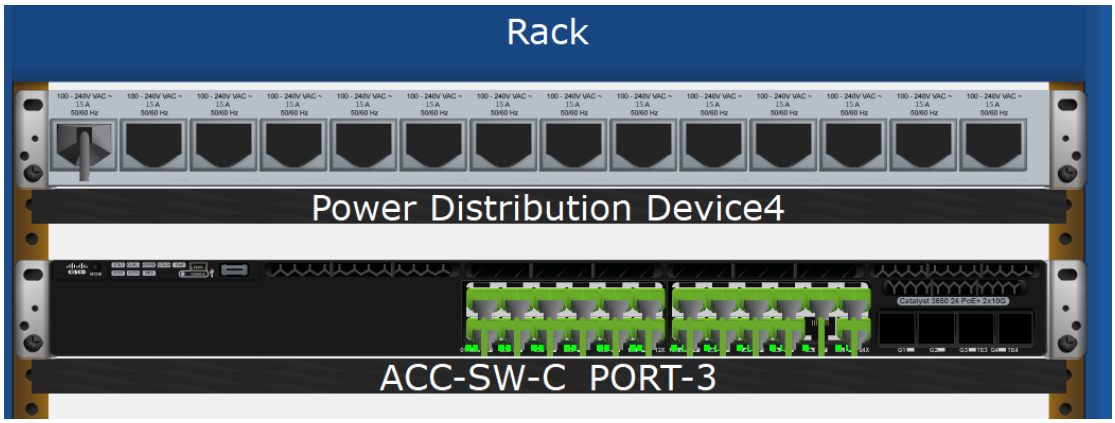
First Floor



Second Floor

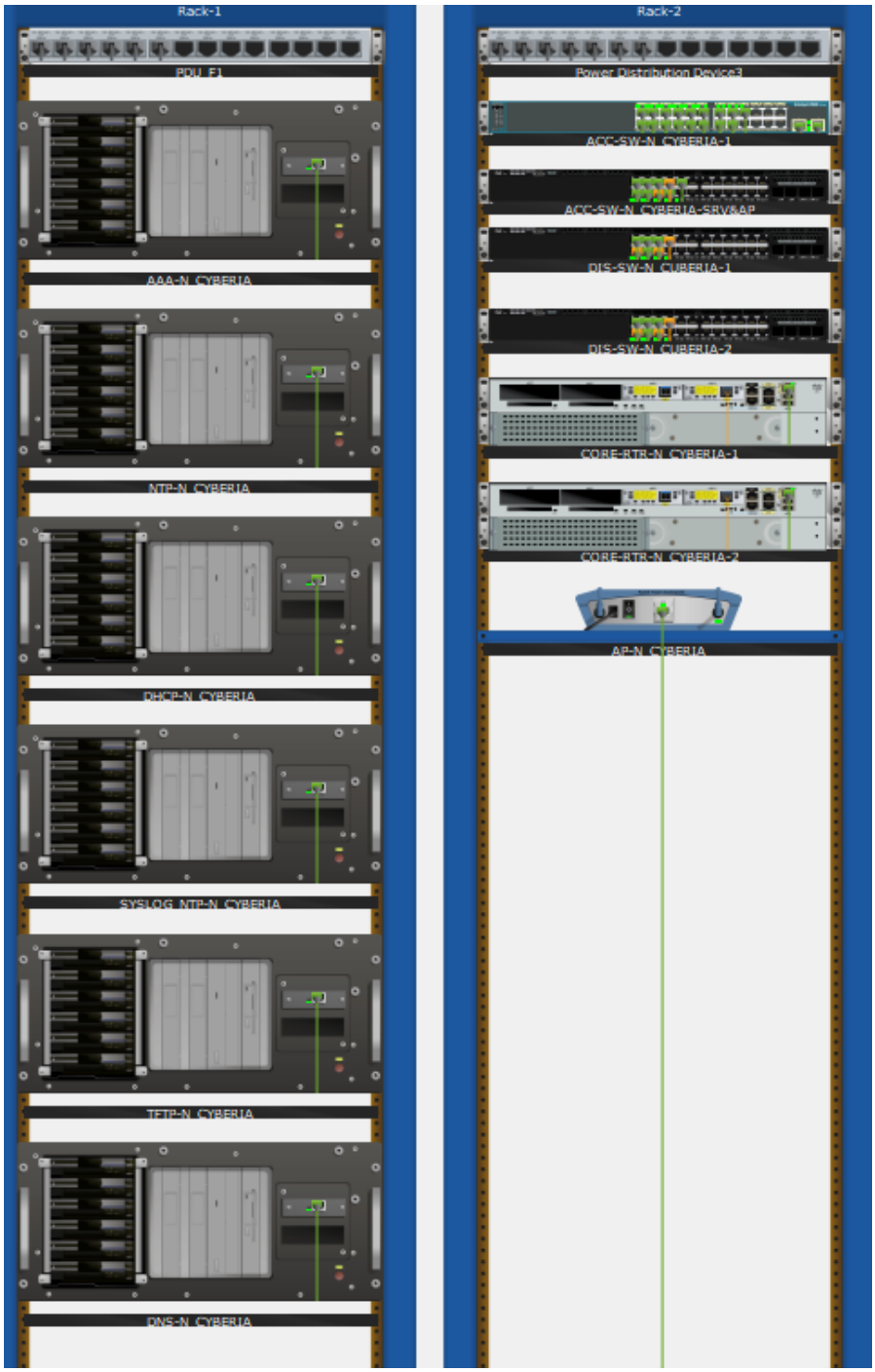


Third Floor

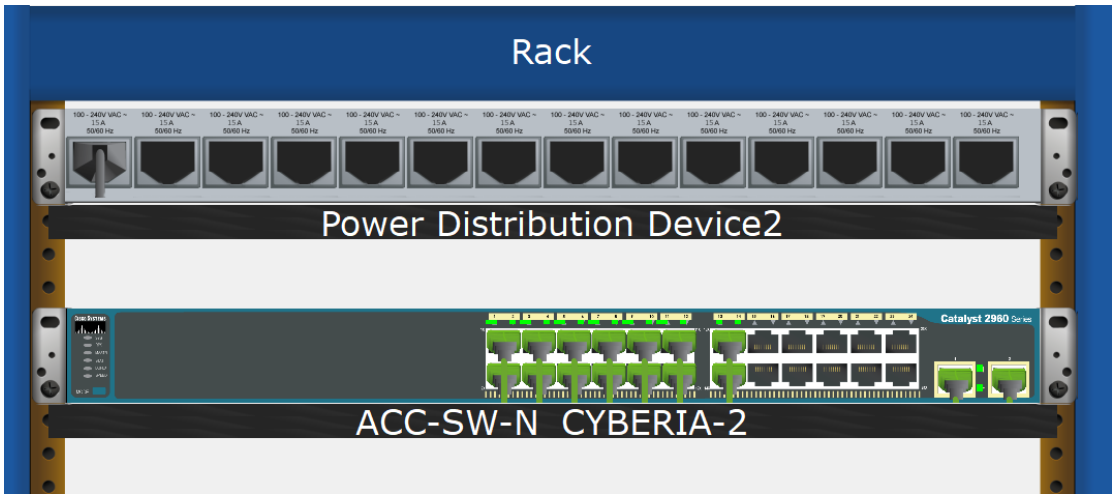


NeoCyberia Branch

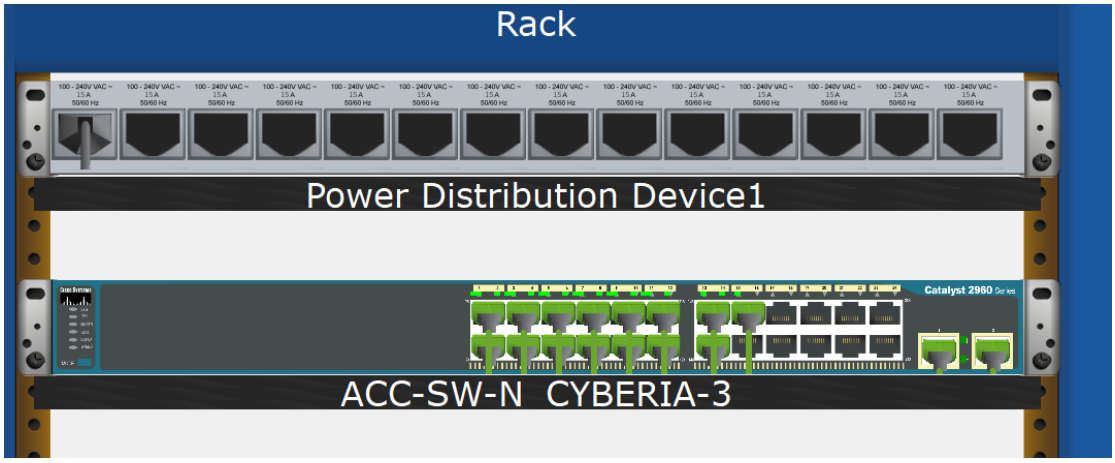
First Floor



Second Floor

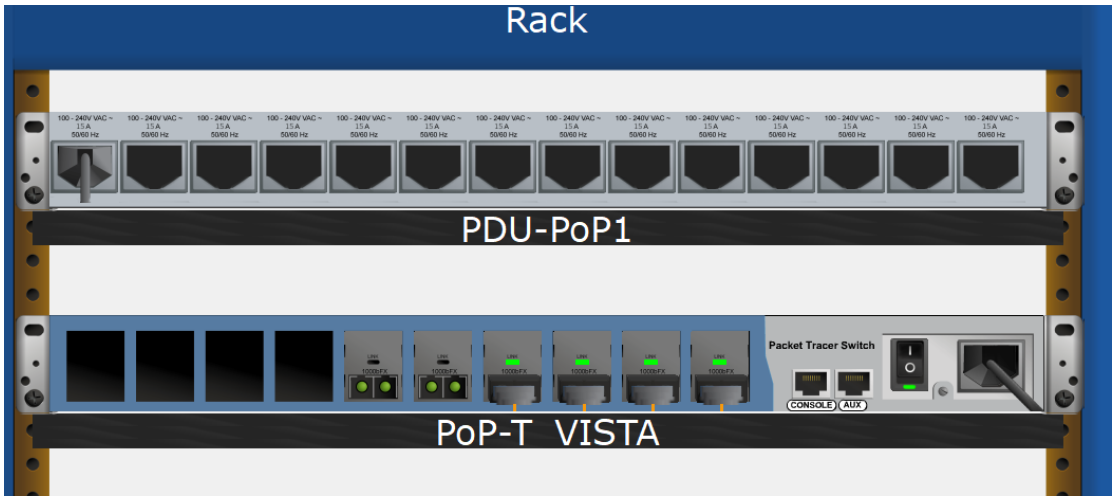


Third Floor

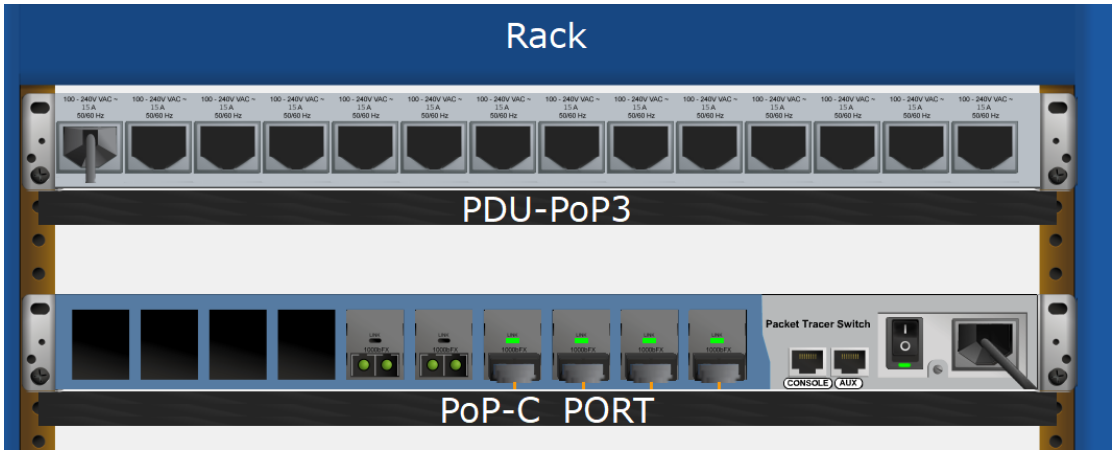


ISP Pops

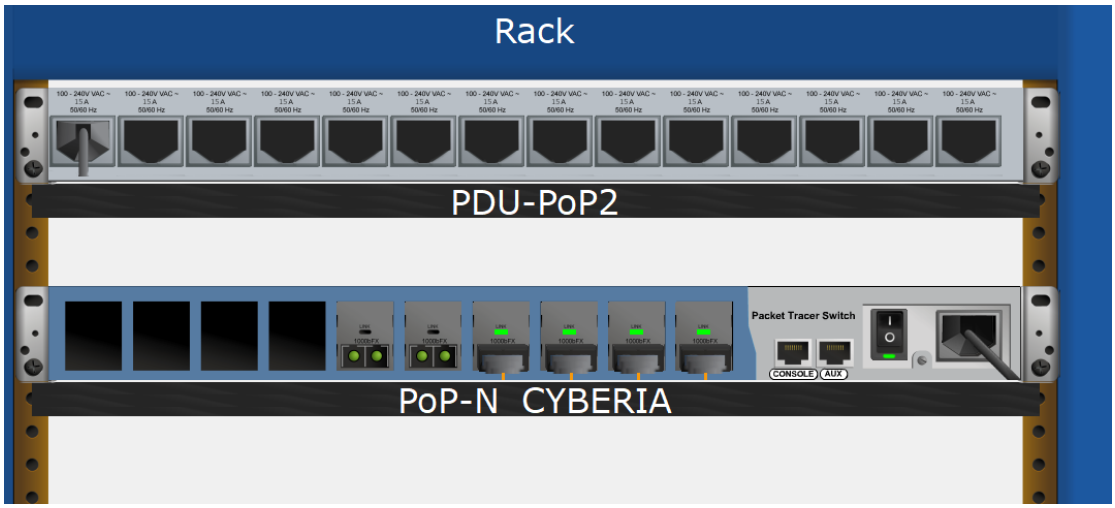
TechVista



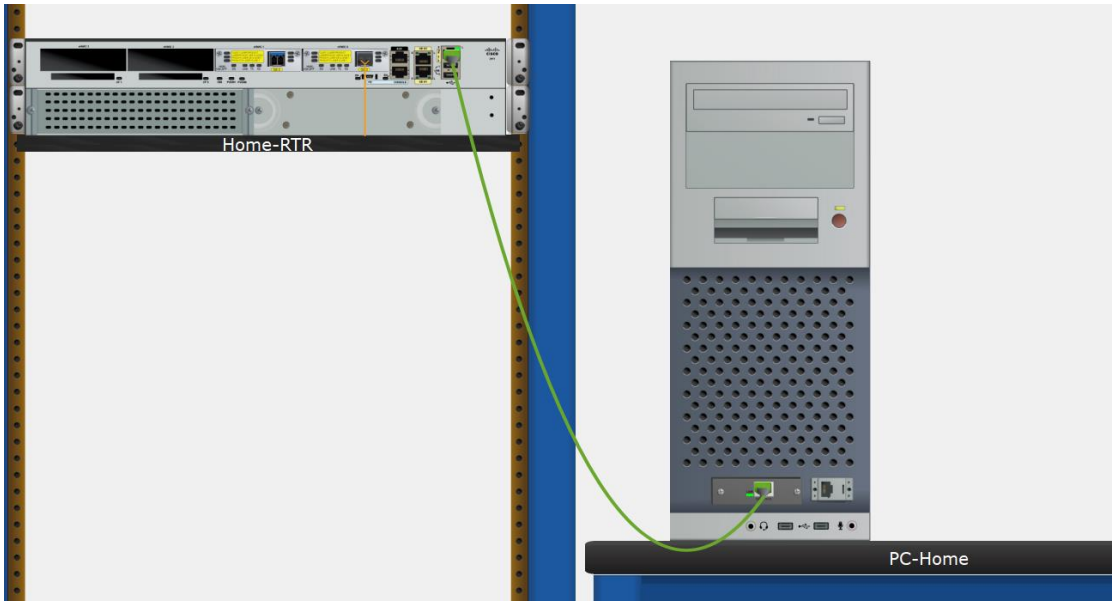
CodePort



NeoCyberia

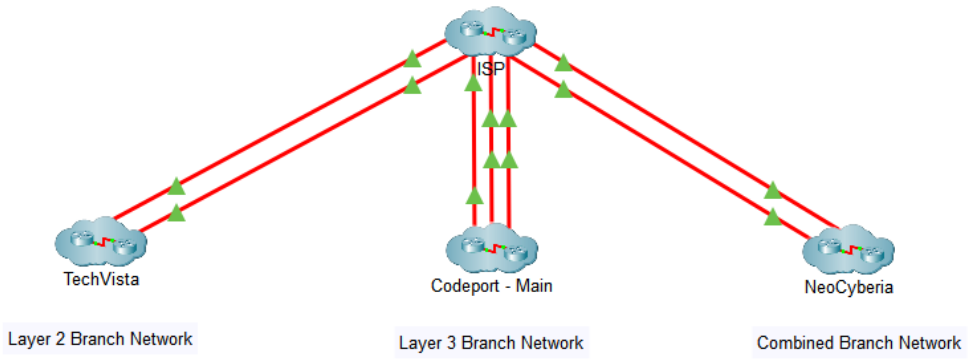


Remote Worker



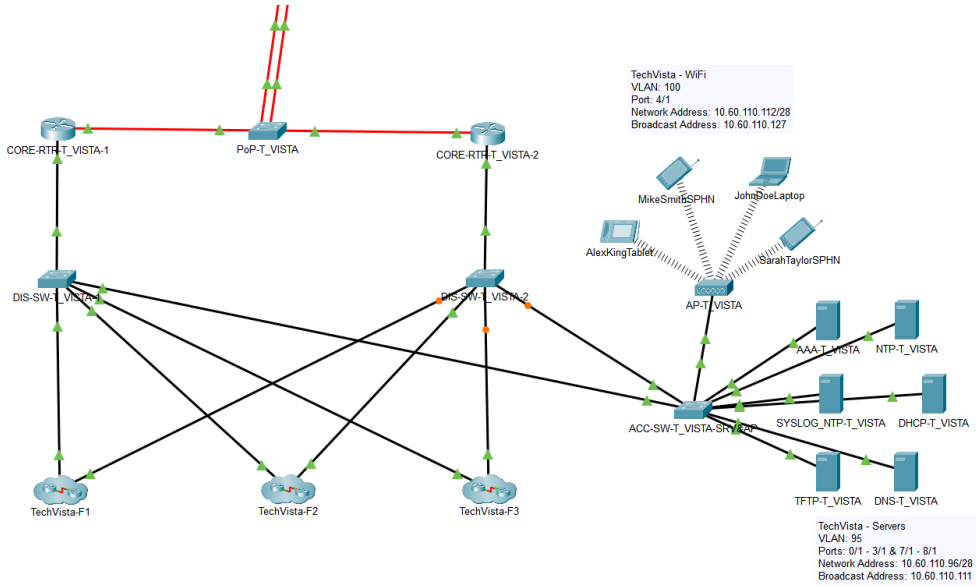
Logical Topology View

Core Network

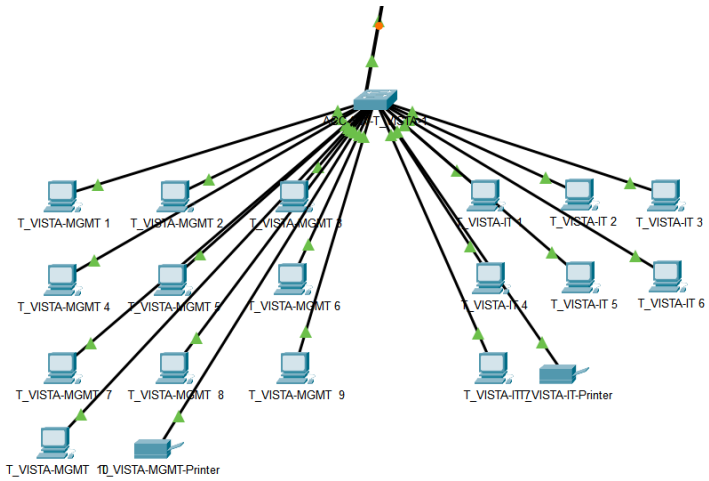


TechVista Branch

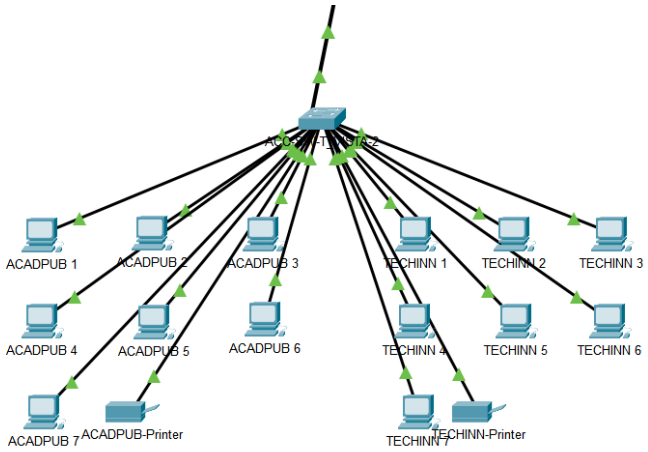
Network Infrastructure



First Floor



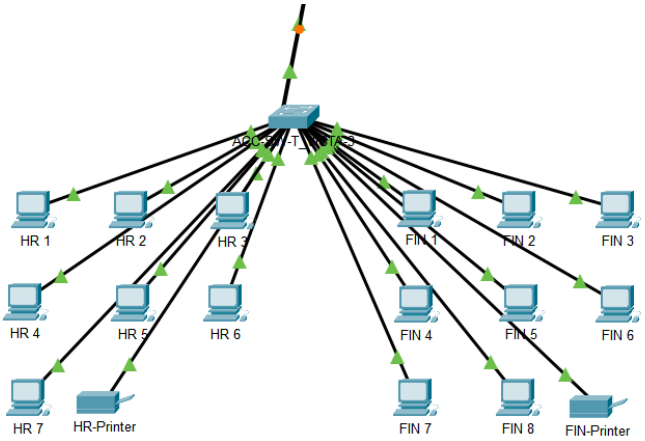
Second Floor



Academic Publishing deparment
VLAN: 75
Ports: 9-16
Network Address: 10.60.110.32/28
Broadcast Address: 10.60.110.47

Technology & Innovation Department
VLAN: 80
Ports: 1-8
Network Address: 10.60.110.48/28
Broadcast Address: 10.60.110.63

Third Floor

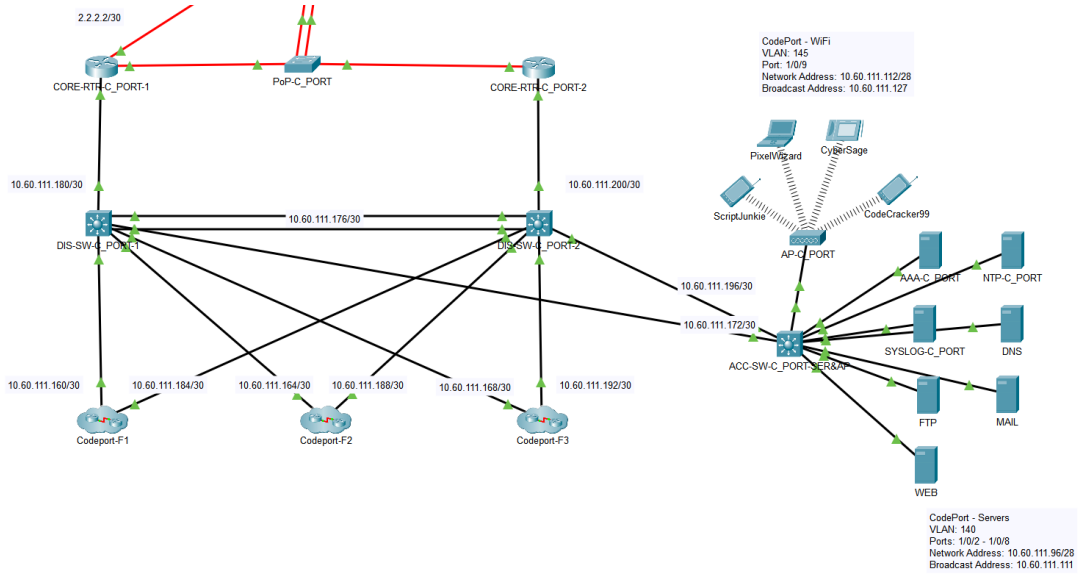


Human Resource Department
VLAN: 85
Ports: 10-17
Network Address: 10.60.110.64/28
Broadcast Address: 10.60.110.79

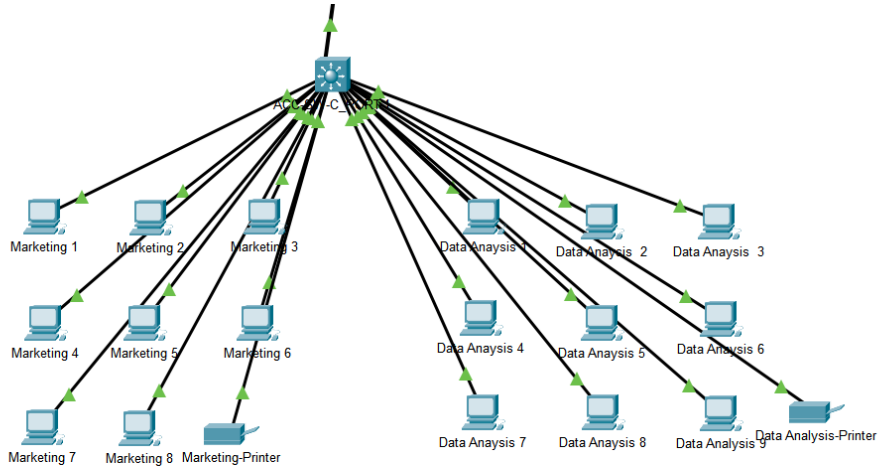
Finance Department
VLAN: 90
Ports: 1-9
Network Address: 10.60.110.80/28
Broadcast Address: 10.60.110.95

CodePort Branch

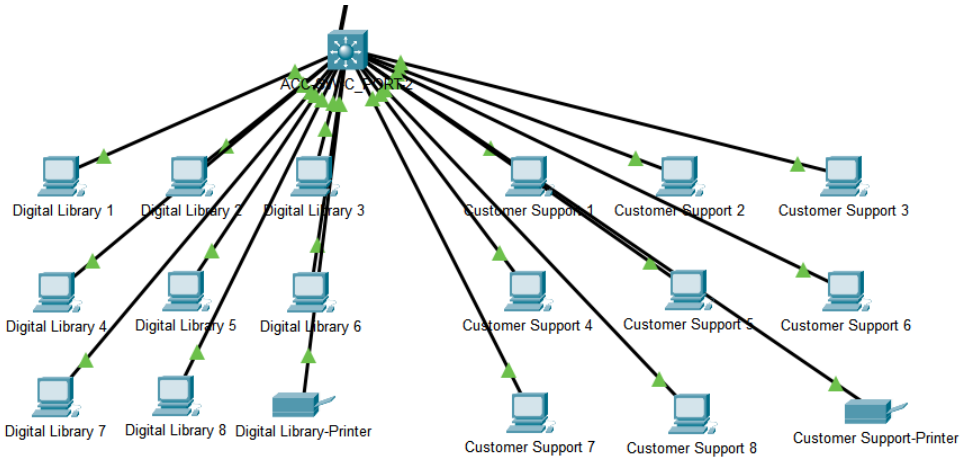
Network Infrastructure



First Floor



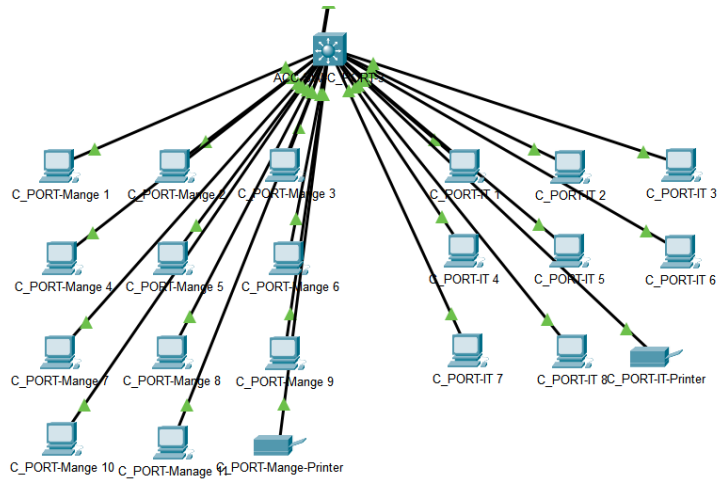
Second Floor



Digital Library Department
VLAN: 120
Ports: 1/0/1 - 1/0/9
Network Address: 10.60.111.32/28
Broadcast Address: 10.60.111.47

Customer Support Department
VLAN: 125
Ports: 1/0/10 -1/0/18
Network Address: 10.60.111.48/28
Broadcast Address: 10.60.111.63

Third Floor

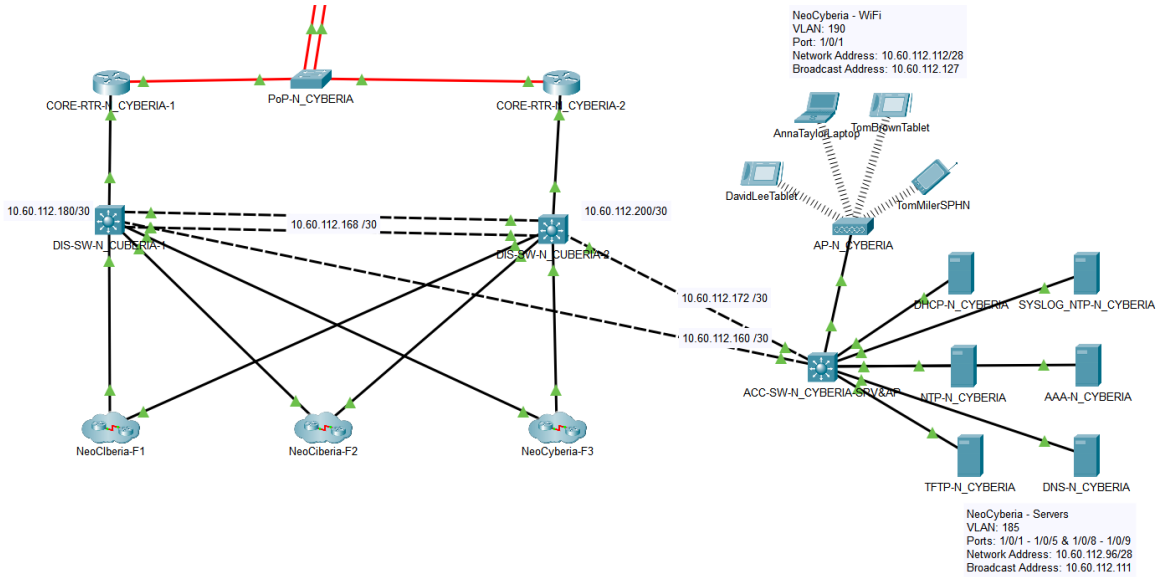


Codeport - Management Department
VLAN: 110
Ports: 1/0/1 - 1/0/12
Network Address: 10.60.111.0/28
Broadcast Address:10.60.111.15

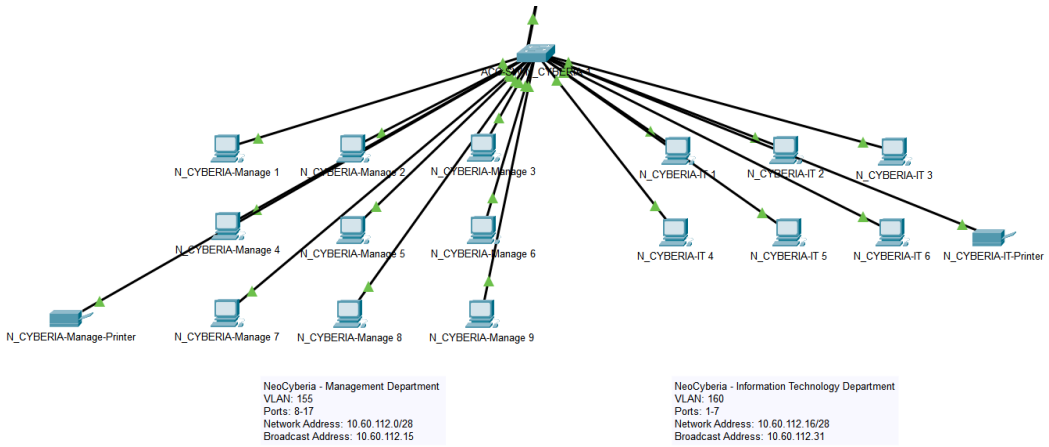
Codeport - Information Technology Department
VLAN: 115
Ports: 1/0/13 - 1/0/21
Network Address: 10.60.111.16/28
Broadcast Address: 10.60.111.31

NeoCyberia Branch

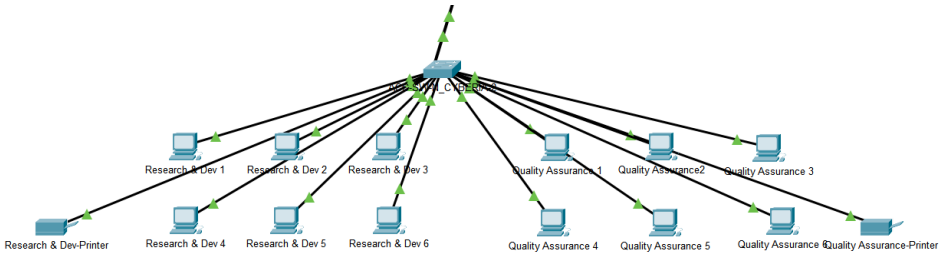
Network Infrastructure



First Floor



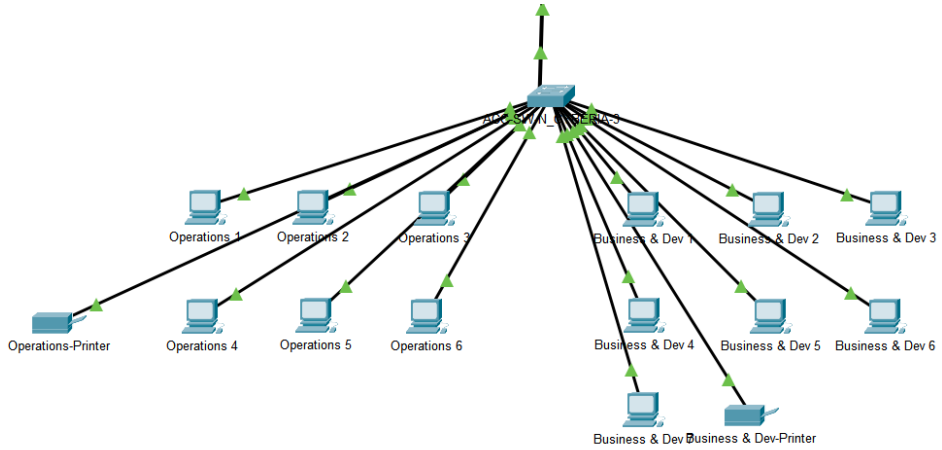
Second Floor



Research & Development Department
VLAN: 165
Ports: 8-14
Network Address: 10.60.112.32/28
Broadcast Address: 10.60.112.47

Quality Assurance Department
VLAN: 170
Ports: 1-7
Network Address: 10.60.112.48/28
Broadcast Address: 10.60.112.63

Third Floor

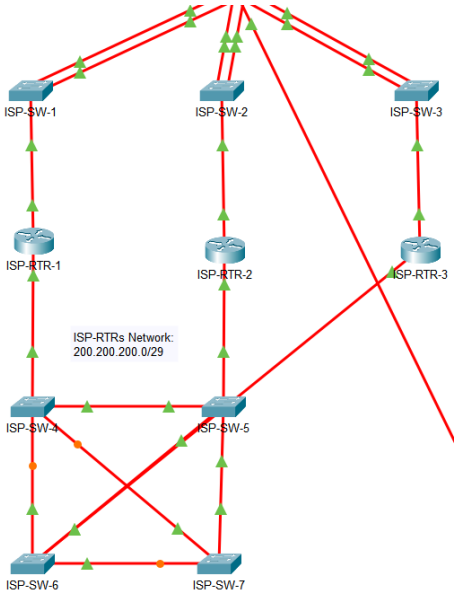


Operations Department
VLAN: 175
Ports: 9-15
Network Address: 10.60.112.64/28
Broadcast Address: 10.60.112.79

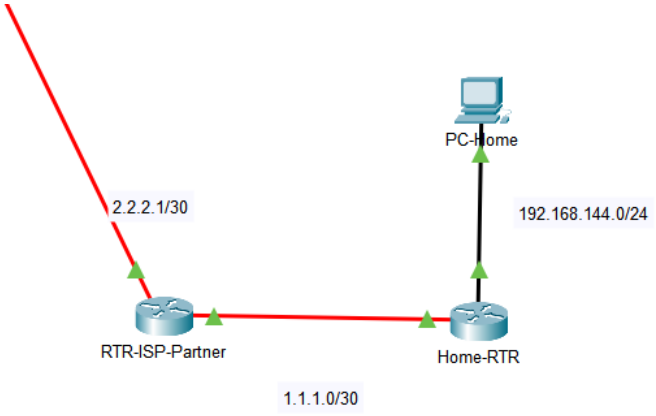
Business & Development Department
VLAN: 180
Ports: 1-8
Network Address: 10.60.112.80/28
Broadcast Address: 10.60.112.95

ISPs

Company-ISP



ISP-Partner



Network Infrastructure and IP Allocation

TechVista Branch

VLAN Routing Allocation Table

Department/Zone Name	VLAN Number	VLAN Name	Network Address	Active Router	Standby Router	Default Gateway
Management	65	TVISTA_MGMT	10.60.110.0/28	10.60.110.12	10.60.110.13	10.60.110.14
Information Technology	70	TVISTA_IT	10.60.110.16/28	10.60.110.28	10.60.110.29	10.60.110.30
Academic Publishing	75	ACADPUB	10.60.110.32/28	10.60.110.44	10.60.110.45	10.60.110.46
Technology & Innovation	80	TECHINN	10.60.110.48/28	10.60.110.60	10.60.110.61	10.60.110.62
Human Resource	85	HR	10.60.110.64/28	10.60.110.76	10.60.110.77	10.60.110.78
Finance	90	FIN	10.60.110.80/28	10.60.110.92	10.60.110.93	10.60.110.94
Servers	95	TVISTA_SRV	10.60.110.96/28	10.60.110.108	10.60.110.109	10.60.110.110
AP	100	TVISTA_AP	10.60.110.112/28	10.60.110.124	10.60.110.125	10.60.110.126
Net Conf	105	TVISTA_NETCONF	10.60.110.128/28	10.60.110.140	10.60.110.141	10.60.110.142

Codeport Branch – Main

VLAN Routing Allocation Table

Department/Zone Name	VLAN Number	VLAN Name	Network Address	Default Gateway
Management	110	CPORT_MGMT	10.60.111.0/28	10.60.111.14
Information Technology	115	CPORT_IT	10.60.111.16/28	10.60.111.30
Digital Library	120	DIGLIB	10.60.111.32/28	10.60.111.46
Customer Support	125	CUSTSUP	10.60.111.48/28	10.60.111.62
Marketing	130	MKTG	10.60.111.64/28	10.60.111.78
Data Analysis	135	DATAAN	10.60.111.80/28	10.60.111.94
Servers	140	CPORT_SRV	10.60.111.96/28	10.60.111.110
AP	145	CPORT_AP	10.60.111.112/28	10.60.111.126

Inter-Device IP Allocation Table

Network Device (ND) 1	Network Device (ND) 2	Network	IP Add - ND 1	IP Add – ND 2
DIS-SW-C_PORT-1	ACC-SW-C_PORT-1	10.60.111.160/30	10.60.111.161	10.60.111.162
DIS-SW-C_PORT-1	ACC-SW-C_PORT-2	10.60.111.164/30	10.60.111.165	10.60.111.166
DIS-SW-C_PORT-1	ACC-SW-C_PORT-3	10.60.111.168/30	10.60.111.169	10.60.111.170
DIS-SW-C_PORT-1	ACC-SW-C_PORT-SRV&AP	10.60.111.172/30	10.60.111.173	10.60.111.174
DIS-SW-C_PORT-1	*DIS-SW-C_PORT-2: EthCha*	10.60.111.176/30	10.60.111.177	10.60.111.178
DIS-SW-C_PORT-1	CORE-RTR -C_PORT-1	10.60.111.180/30	10.60.111.181	10.60.111.182
DIS-SW-C_PORT-2	ACC-SW-C_PORT-1	10.60.111.184/30	10.60.111.185	10.60.111.186
DIS-SW-C_PORT-2	ACC-SW-C_PORT-2	10.60.111.188/30	10.60.111.189	10.60.111.190
DIS-SW-C_PORT-2	ACC-SW-C_PORT-3	10.60.111.192/30	10.60.111.193	10.60.111.194
DIS-SW-C_PORT-2	ACC-SW-C_PORT-SRV&AP	10.60.111.196/30	10.60.111.197	10.60.111.198
DIS-SW-C_PORT-2	*DIS-SW-C_PORT-1: EthCha*	10.60.111.176/30	10.60.111.178	10.60.111.177
DIS-SW-C_PORT-2	CORE-RTR -C_PORT-2	10.60.111.200/30	10.60.111.201	10.60.111.202

NeoCyberia Branch

VLAN Routing Allocation Table

Department/Zone Name	VLAN Number	VLAN Name	Network Address	Active Router	Standby Router	Default Gateway
Management	155	NCYBERIA_MGMT	10.60.112.0/28	10.60.112.12	10.60.112.13	10.60.112.14
Information Technology	160	NCYBERIA_IT	10.60.112.16/28	10.60.112.28	10.60.112.29	10.60.112.30
Research & Development	165	RESDEV	10.60.112.32/28	10.60.112.44	10.60.112.45	10.60.112.46
Quality Assurance	170	QA	10.60.112.48/28	10.60.112.60	10.60.112.61	10.60.112.62
Operations	175	OPS	10.60.112.64/28	10.60.112.76	10.60.112.77	10.60.112.78
Business Development	180	BIZDEV	10.60.112.80/28	10.60.112.92	10.60.112.93	10.60.112.94
Servers	185	NCYBERIA_SRV	10.60.112.96/28	10.60.112.108	10.60.112.109	10.60.112.110
AP	190	NCYBERIA_AP	10.60.112.112/28	10.60.112.124	10.60.112.125	10.60.112.126
Net Conf	195	NCYBERIA_NETCONF	10.60.112.128/28	10.60.112.140	10.60.112.141	10.60.112.142

Inter-Device IP Allocation Table

Network Device (ND) 1	Network Device (ND) 2	Network	IP Add - ND 1	IP Add – ND 2
DIS-SW-N_CYBERIA-1	ACC-SW-N_CYBERIA-SRV&AP	10.60.112.160/30	10.60.112.161	10.60.112.162
DIS-SW-N_CYBERIA-2	ACC-SW-N_CYBERIA-SRV&AP	10.60.112.172/30	10.60.112.173	10.60.112.174
DIS-SW-N_CYBERIA-1	DIS-SW-N_CYBERIA-2 : EthCha	10.60.112.168/30	10.60.112.169	10.60.112.170
DIS-SW-N_CYBERIA-2	DIS-SW-N_CYBERIA-1 : EthCha	10.60.112.168/30	10.60.112.170	10.60.112.169
DIS-SW-N_CYBERIA-1	CORE-RTR-N_CYBERIA-1	10.60.112.180/30	10.60.112.181	10.60.112.182
DIS-SW-N_CYBERIA-2	CORE-RTR-N_CYBERIA-2	10.60.112.200/30	10.60.112.201	10.60.112.202

Equipment Inventory and Access Credentials

TechVista Branch

Equipment Details Table

Hostname	Model	Management IP Address	Physical Location
ACC-SW-T_VISTA-1	2960 IOS15	10.60.110.129	TechVista-F1-Closet
ACC-SW-T_VISTA-2	2960 IOS15	10.60.110.130	TechVista-F2-Closet
ACC-SW-T_VISTA-3	2960 IOS15	10.60.110.131	TechVista-F3-Closet
ACC-SW-T_VISTA-SRV&AP	Empty-PT	10.60.110.132	TechVista-F1-Closet
DIS-SW-T_VISTA-1	Empty-Pt	10.60.110.133	TechVista-F1-Closet
DIS-SW-T_VISTA-2	Empty-Pt	10.60.110.134	TechVista-F1-Closet
CORE-RTR-T_VISTA-1	2911	10.60.110.109	TechVista-F1-Closet
CORE-RTR-T_VISTA-2	2911	10.60.110.110	TechVista-F1-Closet

Equipment Access Credentials Table

Hostname	Enable Password	Enable Secret	VTY Password
ACC-SW-T_VISTA-1	110PASSWORD	110SECRET	AAA Authentication
ACC-SW-T_VISTA-2	110PASSWORD	110SECRET	AAA Authentication
ACC-SW-T_VISTA-3	110PASSWORD	110SECRET	AAA Authentication
ACC-SW-T_VISTA-SRV&AP	110PASSWORD	110SECRET	Login
DIS-SW-T_VISTA-1	110PASSWORD	110SECRET	Login
DIS-SW-T_VISTA-2	110PASSWORD	110SECRET	Login
CORE-RTR-T_VISTA-1	110PASSWORD	110SECRET	AAA Authentication
CORE-RTR-T_VISTA-2	110PASSWORD	110SECRET	AAA Authentication

Codeport Branch - Main

Equipment Details Table

Hostname	Model	Management IP Address	Physical Location
ACC-SW-C_PORT-1	3650-24PS	10.60.111.129	Codeport-F1-Closet
ACC-SW-C_PORT-2	3650-24PS	10.60.111.130	Codeport-F2-Closet
ACC-SW-C_PORT-3	3650-24PS	10.60.111.131	Codeport-F3-Closet
ACC-SW-C_PORT-SRV&AP	3650-24PS	10.60.111.132	Codeport-F1-Closet
DIS-SW-C_PORT-1	3650-24PS	10.60.111.133	Codeport-F1-Closet
DIS-SW-C_PORT-2	3650-24PS	10.60.111.134	Codeport-F1-Closet
CORE-RTR-C_PORT-1	2911	10.60.111.135	Codeport-F1-Closet
CORE-RTR-C_PORT-2	2911	10.60.111.136	Codeport-F1-Closet

Equipment Access Credentials Table

Hostname	Enable Password	Enable Secret	VTY Password
ACC-SW-C_PORT-1	111SPASSWORD	111SECRET	AAA Authentication
ACC-SW-C_PORT-2	111SPASSWORD	111SECRET	AAA Authentication
ACC-SW-C_PORT-3	111SPASSWORD	111SECRET	AAA Authentication
ACC-SW-C_PORT-SRV&AP	111SPASSWORD	111SECRET	AAA Authentication
DIS-SW-C_PORT-1	111SPASSWORD	111SECRET	AAA Authentication
DIS-SW-C_PORT-2	111SPASSWORD	111SECRET	AAA Authentication
CORE-RTR-C_PORT-1	111SPASSWORD	111SECRET	AAA Authentication
CORE-RTR-C_PORT-2	111SPASSWORD	111SECRET	AAA Authentication

NeoCyberia Branch

Equipment Details Table

Hostname	Model	Management IP Address	Physical Location
ACC-SW-N_CYBERIA-1	2960 IOS15	10.60.112.129	NeoCyberia-F1-Closet
ACC-SW-N_CYBERIA-2	2960 IOS15	10.60.112.130	NeoCyberia-F2-Closet
ACC-SW-N_CYBERIA-3	2960 IOS15	10.60.112.131	NeoCyberia-F3-Closet
ACC-SW-N_CYBERIA-SRV&AP	3650-24PS	10.60.112.132	NeoCyberia-F1-Closet
DIS-SW-N_CYBERIA-1	3650-24PS	10.60.112.133	NeoCyberia-F1-Closet
DIS-SW-N_CYBERIA-2	3650-24PS	10.60.112.134	NeoCyberia-F1-Closet
CORE-RTR-N_CYBERIA-1	2911	10.60.112.135	NeoCyberia-F1-Closet
CORE-RTR-N_CYBERIA-2	2911	10.60.112.136	NeoCyberia-F1-Closet

Equipment Access Credentials Table

Hostname	Enable Password	Enable Secret	VTY Password
ACC-SW-N_CYBERIA-1	112PASSWORD	112SECRET	AAA Authentication
ACC-SW-N_CYBERIA-2	112PASSWORD	112SECRET	AAA Authentication
ACC-SW-N_CYBERIA-3	112PASSWORD	112SECRET	AAA Authentication
ACC-SW-N_CYBERIA-SRV&AP	112PASSWORD	112SECRET	AAA Authentication
DIS-SW-N_CYBERIA-1	112PASSWORD	112SECRET	AAA Authentication
DIS-SW-N_CYBERIA-2	112PASSWORD	112SECRET	AAA Authentication
CORE-RTR-N_CYBERIA-1	112PASSWORD	112SECRET	AAA Authentication
CORE-RTR-N_CYBERIA-2	112PASSWORD	112SECRET	AAA Authentication

Servers Config and Domain Mappings

TechVista Branch

Server	Address	Domain
AAA	10.60.110.97	aaa.techvista.mentoranexus.com
NTP	10.60.110.98	ntp.techvista.mentoranexus.com
SYSLOG_NTP	10.60.110.99	syslog.techvista.mentoranexus.com
DHCP	10.60.110.100	N/A
TFTP	10.60.110.101	tftp.techvista.mentoranexus.com
DNS	10.60.110.102	N/A

Codeport Branch - Main

Server	Address	Domain
AAA	10.60.111.97	aaa.mentoranexus.com
NTP	10.60.111.98	ntp.mentoranexus.com
SYSLOG	10.60.111.99	syslog.mentoranexus.com
DNS	10.60.111.100	N/A
FTP	10.60.111.101	ftp.mentoranexus.com
MAIL	10.60.111.102	mail.mentoranexus.com
WEB (HTTP)	10.60.111.103	mentoranexus.com

NeoCyberia Branch

Server	Address	Domain
DHCP	10.60.112.97	N/A
SYSLOG_NTP	10.60.112.98	syslog.neocyberia.mentoranexus.com
NTP	10.60.112.99	ntp.neocyberia.mentoranexus.com
AAA	10.60.112.100	aaa.neocyberia.mentoranexus.com
TFTP	10.60.112.101	tftp.neocyberia.mentoranexus.com
DNS	10.60.112.102	N/A

AAA Tables

TechVista Branch

Hostname	Host Address	Key	Server Type
ACC-SW-T_VISTA-1	10.60.110.129	110TACACS	Tacacs
ACC-SW-T_VISTA-2	10.60.110.130	110TACACS	Tacacs
ACC-SW-T_VISTA-3	10.60.110.131	110TACACS	Tacacs
ACC-SW-T_VISTA-SRV&AP	10.60.110.132	Not Supported	Not Supported
DIS-SW-T_VISTA-1	10.60.110.133	Not Supported	Not Supported
DIS-SW-T_VISTA-2	10.60.110.134	Not Supported	Not Supported
CORE-RTR-T_VISTA-1	10.60.110.109	110TACACS	Tacacs
CORE-RTR-T_VISTA-2	10.60.110.110	110TACACS	Tacacs

Codeport Branch - Main

Hostname	Host Address	Key	Server Type
ACC-SW-C_PORT-1	10.60.111.186	111TACACS	Tacacs
ACC-SW-C_PORT-2	10.60.111.190	111TACACS	Tacacs
ACC-SW-C_PORT-3	10.60.111.194	111TACACS	Tacacs
ACC-SW-C_PORT-SRV&AP	10.60.111.198	111TACACS	Tacacs
DIS-SW-C_PORT-1	10.60.111.173	111TACACS	Tacacs
DIS-SW-C_PORT-2	10.60.111.197	111TACACS	Tacacs
CORE-RTR-C_PORT-1	10.60.111.182	111TACACS	Tacacs
CORE-RTR-C_PORT-2	10.60.111.202	111TACACS	Tacacs

NeoCyberia Branch

Hostname	Host Address	Key	Server Type
ACC-SW-N_CYBERIA -1	10.60.112.129	112TACACS	Tacacs
ACC-SW-N_CYBERIA -2	10.60.112.130	112TACACS	Tacacs
ACC-SW-N_CYBERIA -3	10.60.112.131	112TACACS	Tacacs
ACC-SW-N_CYBERIA-SRV&AP	10.60.112.110	112TACACS	Tacacs
DIS-SW-N_CYBERIA -1	10.60.112.161	112TACACS	Tacacs
DIS-SW-N_CYBERIA -2	10.60.112.173	112TACACS	Tacacs
CORE-RTR-N_CYBERIA-1	10.60.112.182	112TACACS	Tacacs
CORE-RTR-N_CYBERIA-2	10.60.112.202	112TACACS	Tacacs

VTP Tables

TechVista Branch

Hostname	Role	Domain-Name	Password
ACC-SW-T_VISTA-1	client	mentoranexus.com	vtp1234
ACC-SW-T_VISTA-2	client	mentoranexus.com	vtp1234
ACC-SW-T_VISTA-3	client	mentoranexus.com	vtp1234
ACC-SW-T_VISTA-SRV&AP	client	mentoranexus.com	vtp1234
DIS-SW-T_VISTA-1	server	mentoranexus.com	vtp1234
DIS-SW-T_VISTA-2	server	mentoranexus.com	vtp1234

NeoCyberia Branch

Hostname	Role	Domain-Name	Password
ACC-SW-N_CYBERIA -1	client	mentoranexus.com	vtp1234
ACC-SW- N_CYBERIA -2	client	mentoranexus.com	vtp1234
ACC-SW- N_CYBERIA -3	client	mentoranexus.com	vtp1234
ACC-SW- N_CYBERIA -SRV&AP	client	mentoranexus.com	vtp1234
DIS-SW- N_CYBERIA -1	server	mentoranexus.com	vtp1234
DIS-SW- N_CYBERIA -2	server	mentoranexus.com	vtp1234

AP Tables

Hostname	SSID	Password
AP-T_VISTA	TechVistaWiFi	110WIFIPASS
AP-C_PORT	CodePortWIFi	111WIFIPASS
AP-N_CYBERIA	NeoCyberiaWiFi	112WIFIPASS

Mail Tables

Domain Name - *mail.mentoranexus.com*

TechVista Branch

User Name	Password	Department	Hostname
Alexander	AlexanderMail1234	Management	T_VISTA-MGMT 1
Andrew	AndrewMail1234	IT	T_VISTA-IT 1
Anthony	AnthonyMail1234	Academic Publishing	ACADPUB 1
Brian	BrianMail1234	Technology & Innovation	TECHINN 1
Daniel	DanielMail1234	HR	HR 1
Amy	AmyMail1234	Finance	FIN 1

Employee Name	Official Email Address
Alexander Carter	alexander@mail.mentoranexus.com
Andrew Mitchell	andrew@mail.mentoranexus.com
Anthony Roberts	anthony@mail.mentoranexus.com
Brian Thompson	brian@mail.mentoranexus.com
Daniel Harrison	daniel@mail.mentoranexus.com
Amy Richardton	amy@mail.mentoranexus.com

CodePort Branch

User Name	Password	Department	Hostname
Betty	BettyMail1234	Management	C_PORT-Manage 1
Carol	CarolMail1234	IT	C_PORT_IT 1
Emma	EmmaMail1234	Digital Library	Digital Library 1
Lisa	LisaMail1234	Customer Support	Customer Support 1
Mark	MarkMail1234	Marketing	Marketing 1
Paul	PaulMail1234	Data Analysis	Data Analysis 1

Employee Name	Official Email Address
Betty Colins	betty@mail.mentoranexus.com
Carol Simmons	carol@mail.mentoranexus.com
Emma Wright	emma@mail.mentoranexus.com
Lisa Andreson	lisa@mail.mentoranexus.com
Mark Bennett	mark@mail.mentoranexus.com
Paul Reynolds	paul@mail.mentoranexus.com

NeoCyberia Branch

User Name	Password	Department	Hostname
Robert	RobertMail1234	Management	N_CYBERIA-Manage 1
Ryan	RyanMail1234	IT	N_CYBERIA-IT 1
Scott	ScottMail1234	Research & Dev	Research & Dev 1
Steven	StevenMail1234	Quality Assurance	Quality Assurance 1
Thomas	ThomasMail1234	Operations	Operations 1
Jose	JoseMail1234	Business Development	Business & Dev 1

Employee Name	Official Email Address
Robert Phillips	robert@mail.mentoranexus.com
Ryan Edwards	ryan@mail.mentoranexus.com
Scott Douglas	scott@mail.mentoranexus.com
Steven Foster	steven@mail.mentoranexus.com
Thomas Griffin	thomas@mail.mentoranexus.com
Jose Martinez	jose@mail.mentoranexus.com

BGP Peer and ISP Network Topology

BGP Peer Relationships Table

Network Subnet	ASN	IP Address	Neighbor IP Addresses	Neighbor ASNs
200.200.200.0/29	10	200.200.200.1	200.200.200.2	20
			200.200.200.3	30
	20	200.200.200.2	200.200.200.1	10
			200.200.200.3	30
	30	200.200.200.3	200.200.200.1	10
			200.200.200.2	20

Branch ISP Connectivity and IP Allocation

Config Parameter	TechVista Site	CodePort Site	NeoCyberia Site
Subnet	110.110.110.0/29	111.111.111.0/29	112.112.112.0/29
ISP Router ASN	10	20	30
Core Router 1	CORE-RTR-T_VISTA-1	CORE-RTR-C_PORT-1	CORE-RTR-N_CYBERIA-1
Core Router 2	CORE-RTR-T_VISTA-2	CORE-RTR-C_PORT-2	CORE-RTR-N_CYBERIA-2
ISP Router	ISP-RTR-1	ISP-RTR-2	ISP-RTR-3
Allocated IP 1	.1	.1	.1
Allocated IP 2	.2	.2	.2
Allocated IP 3	.3	.3	.3

Secure Tunneling and Endpoint Configuration

TechVista

Tunnel Endpoint Router and Public Interface Config

Tunnel ID	Source Router	Destination Router	Source Interface / IP Address	Destination IP Address
11011101	CORE-RTR-T_VISTA-1	CORE-RTR-C_PORT-1	G0/0/0 110.110.110.1	111.111.111.1
11011201	CORE-RTR-T_VISTA-1	CORE-RTR-N_CYBERIA-1	G0/0/0 110.110.110.1	112.112.112.1
11011102	CORE-RTR-T_VISTA-2	CORE-RTR-C_PORT-2	G0/0/0 110.110.110.2	111.111.111.2
11011202	CORE-RTR-T_VISTA-2	CORE-RTR-N_CYBERIA-2	G0/0/0 110.110.110.2	112.112.112.2

Tunnel ID and Subnet Assignment

Tunnel ID	IP Subnet	Local Tunnel Endpoint	Remote Tunnel Endpoint
11011101	192.168.1.0/30	192.168.1.1	192.168.1.2
11011201	192.168.1.4/30	192.168.1.5	192.168.1.6
11011102	192.168.1.8/30	192.168.1.9	192.168.1.10
11011202	192.168.1.12/30	192.168.1.13	192.168.1.14

CodePort

Tunnel Endpoint Router and Public Interface Config

Tunnel ID	Source Router	Destination Router	Source Interface / IP Address	Destination IP Address
11111001	CORE-RTR-C_PORT-1	CORE-RTR-T_VISTA-1	G0/0/0 111.111.111.1	110.110.110.1
11111201	CORE-RTR-C_PORT-1	CORE-RTR-N_CYBERIA-1	G0/0/0 111.111.111.1	112.112.112.1
11111002	CORE-RTR-C_PORT-2	CORE-RTR-T_VISTA-2	G0/0/0 111.111.111.2	110.110.110.2
11111202	CORE-RTR-C_PORT-2	CORE-RTR-N_CYBERIA-2	G0/0/0 111.111.111.2	112.112.112.2

Tunnel ID and Subnet Assignment

Tunnel ID	IP Subnet	Local Tunnel Endpoint	Remote Tunnel Endpoint
11111001	192.168.1.0/30	192.168.1.2	192.168.1.1
11111201	192.168.1.16/30	192.168.1.17	192.168.1.18
11111002	192.168.1.8/30	192.168.1.10	192.168.1.9
11111202	192.168.1.20/30	192.168.1.21	192.168.1.22

NeoCyberia

Tunnel Endpoint Router and Public Interface Config

Tunnel ID	Source Router	Destination Router	Source Interface / IP Address	Destination IP Address
11211001	CORE-RTR-N_CYBERIA-1	CORE-RTR-T_VISTA-1	G0/0/0 112.112.112.1	110.110.110.1
11211101	CORE-RTR-N_CYBERIA-1	CORE-RTR-C_PORT-1	G0/0/0 112.112.112.1	111.111.111.1
11211002	CORE-RTR-N_CYBERIA-2	CORE-RTR-T_VISTA-2	G0/0/0 112.112.112.2	110.110.110.2
11211102	CORE-RTR-N_CYBERIA-2	CORE-RTR-C_PORT-2	G0/0/0 112.112.112.2	111.111.111.2

Tunnel ID and Subnet Assignment

Tunnel ID	IP Subnet	Local Tunnel Endpoint	Remote Tunnel Endpoint
11211001	192.168.1.4/30	192.168.1.6	192.168.1.5
11211101	192.168.1.16/30	192.168.1.18	192.168.1.17
11211002	192.168.1.12/30	192.168.1.14	192.168.1.13
11211102	192.168.1.20/30	192.168.1.22	192.168.1.21

IPSec VPN Device Configuration

Phase 1: ISKAMP/IKE Configuration

Defines encryption and hashing algorithms, authentication method, and key exchange parameters for establishing the secure tunnel

Device	Policy Number	Encryption	Hash	Authentication	DH Group	Lifetime
CORE-RTR-T_VISTA-1	10	aes 256	sha	pre-share	5	86400
CORE-RTR-T_VISTA-2	10	aes 256	sha	pre-share	5	86400
CORE-RTR-C_PORT-1	10	aes 256	sha	pre-share	5	86400
CORE-RTR-C_PORT-2	10	aes 256	sha	pre-share	5	86400
CORE-RTR-N_CYBERIA-1	10	aes 256	sha	pre-share	5	86400
CORE-RTR-N_CYBERIA-2	10	aes 256	sha	pre-share	5	86400
CORE-RTR-T_VISTA-1	10	aes 256	sha	pre-share	5	86400

Phase 2: IPSec Configuration

Defines IPSec Security Associations, transform sets, and access lists for encryption.

Note: the ISKAMP Key belongs to Phase 1 despite its present in this Phase 2 subsection.

Device	ISAKMP Key	Peers	Transform Set Name
CORE-RTR-T_VISTA-1	MentoraKey	111.111.111.1, 112.112.112.1	[T_V1=>C_P1,N_C1]_SET
CORE-RTR-T_VISTA-2	MentoraKey	111.111.111.2, 112.112.112.2	[T_V2=>C_P2,N_C2]_SET
CORE-RTR-C_PORT-1	MentoraKey	110.110.110.1, 112.112.112.1	[C_P1=>T_V1,N_C1]_SET
CORE-RTR-C_PORT-2	MentoraKey	110.110.110.2, 112.112.112.2	[C_P2=>T_V2,N_C2]_SET
CORE-RTR-N_CYBERIA-1	MentoraKey	110.110.110.1, 111.111.111.1	[N_C1=>T_V1,C_P1]_SET
CORE-RTR-N_CYBERIA-2	MentoraKey	110.110.110.2, 111.111.111.2	[N_C2=>T_V2,C_P2]_SET

Device	Access List Rules	Crypto Maps	Interface
CORE-RTR-T_VISTA-1	10.60.110.0/24 -> 10.60.111.0/24, 10.60.110.0/24 -> 10.60.112.0/24	[T_V1=>C_P1]_MAP 10, [T_V1=>N_C1]_MAP 20	G0/0/0
CORE-RTR-T_VISTA-2	10.60.110.0/24 -> 10.60.111.0/24, 10.60.110.0/24 -> 10.60.112.0/24	[T_V2=>C_P2]_MAP 10, [T_V2=>N_C2]_MAP 20	G0/0/0
CORE-RTR-C_PORT-1	10.60.111.0/24 -> 10.60.110.0/24, 10.60.111.0/24 -> 10.60.112.0/24	[C_P1=>T_V1]_MAP 10, [C_P1=>N_C1]_MAP 20	G0/0/0
CORE-RTR-C_PORT-2	10.60.111.0/24 -> 10.60.110.0/24, 10.60.111.0/24 -> 10.60.112.0/24	[C_P2=>T_V2]_MAP 10, [C_P2=>N_C2]_MAP 20	G0/0/0
CORE-RTR-N_CYBERIA-1	10.60.112.0/24 -> 10.60.110.0/24, 10.60.112.0/24 -> 10.60.111.0/24	[N_C1=>T_V1]_MAP 10, [N_C1=>C_P1]_MAP 20	G0/0/0
CORE-RTR-N_CYBERIA-2	10.60.112.0/24 -> 10.60.110.0/24, 10.60.112.0/24 -> 10.60.111.0/24	[N_C2=>T_V2]_MAP 10, [N_C2=>C_P2]_MAP 20	G0/0/0

Servers Configuration

Domain Name System (DNS)

DNS translates human-readable **domain and host names** into **numeric IP addresses** using a **distributed, hierarchical structure** consisting of **root servers**, **top-level domain (TLD) servers**, and **authoritative name servers**. The resolution process involves **recursive queries** (handled by resolvers) and **iterative lookups** (performed by **DNS servers**). DNS supports **resource records** such as **A** (IPv4), **AAAA** (IPv6), **CNAME** (alias), **MX** (mail exchange), and **TXT** (arbitrary text storage).

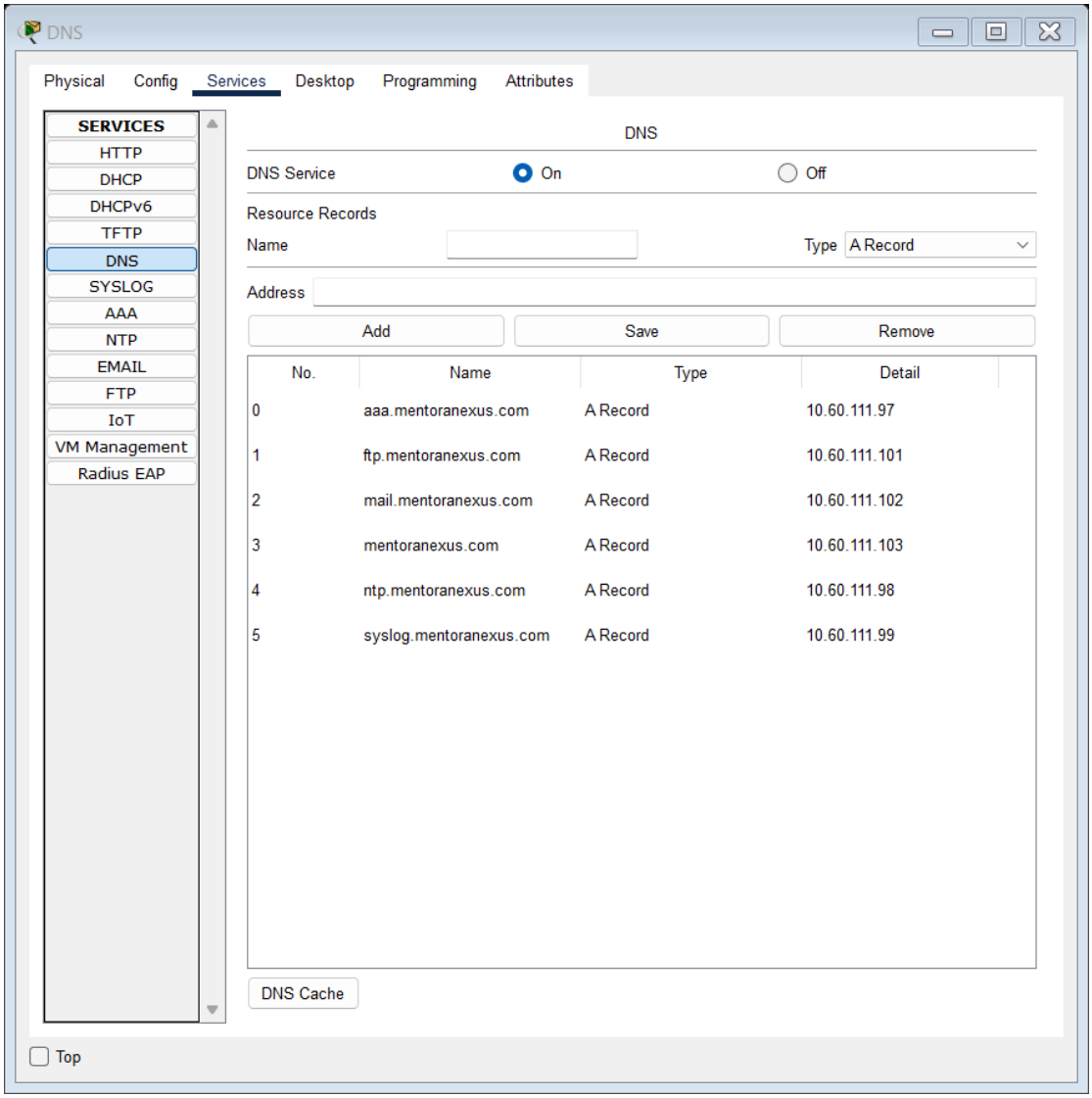
Uses **UDP port 53** for standard queries**; TCP port 53** is used for large responses and zone transfers.

IOS Commands Alongside Their Descriptions:

Command	Description
[no] ip domain lookup	[Disables] enables resolution of unknown issued strings by a remote DNS server
ip name-server *dns_server_ip_address*	Specifies the DNS server for performing the name resolutions.

Sample execution of specified commands

CORE-RTR-T_VISTA-1(config)#ip domain lookup
CORE-RTR-T_VISTA-1(config)#ip name-server 10.60.110.102

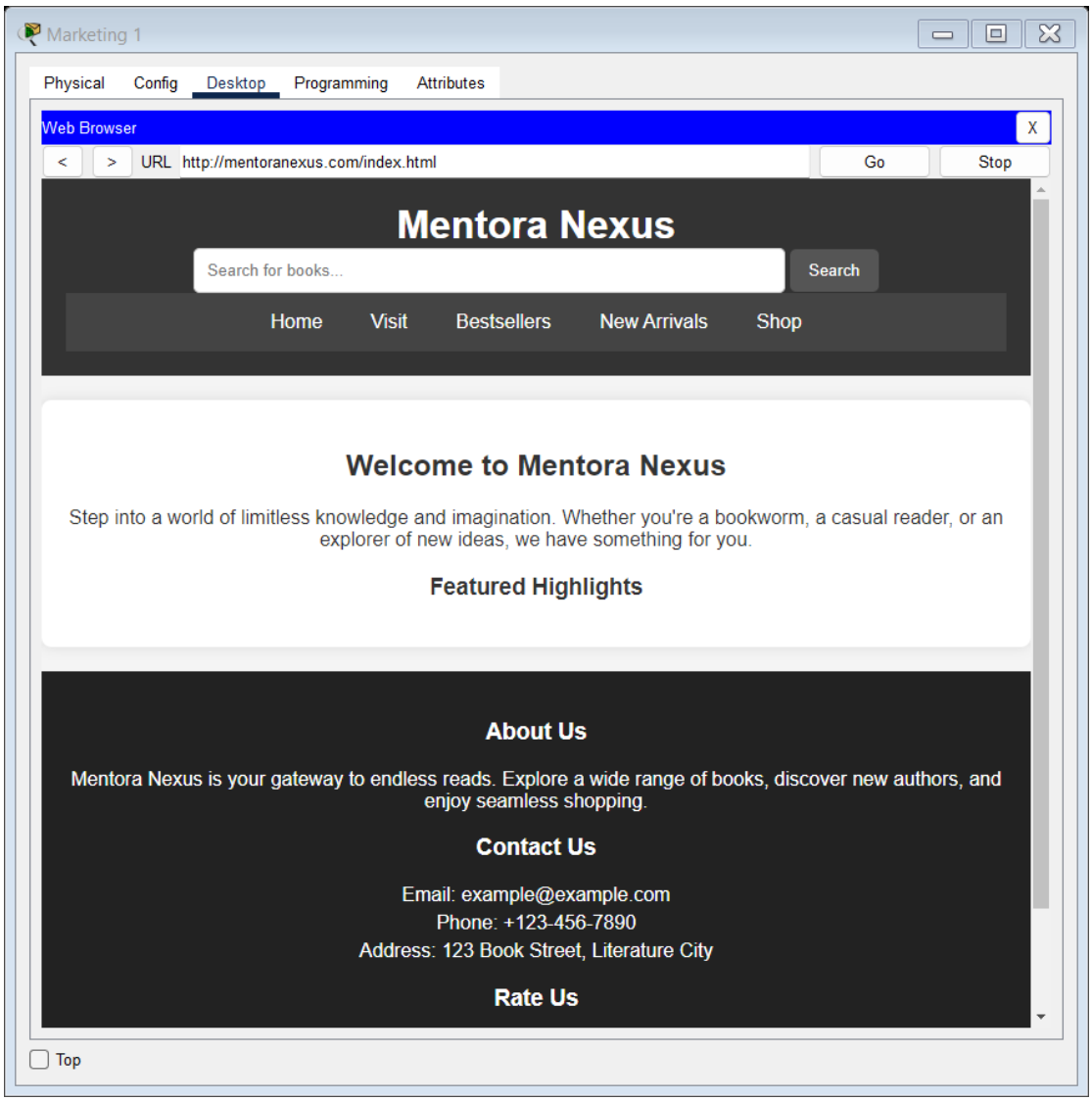


Screenshot x.x — Codeport's DNS server configuration instance.

Hypertext Transfer Protocol (HTTP/HTTPS)

HTTP defines the **stateless** communication model between **clients** (web browsers) and **web servers**, using request methods such as **GET, POST**, **PUT**, and **DELETE**. **HTTPS** incorporates **TLS/SSL encryption** to ensure **data confidentiality, integrity,** and **authenticity**. The **handshake process** establishes secure connections using **asymmetric encryption** before exchanging encrypted session data.

HTTP operates on **TCP port 80**; **HTTPS** uses **TCP port 443** for encrypted transmissions.



Screenshot x.x — PC accesses mentoranexus.com through Codeport's HTTP server.

File Transfer Protocol (FTP)

FTP facilitates **file exchanges** over a **client-server architecture** with dedicated **control** and **data** channels. **Active mode** initiates data transfer from the server to the client's specified port, while **passive mode** allows clients to establish the connection. FTP lacks inherent encryption but can be secured via **FTPS** (SSL/TLS) or **SFTP** (SSH-based).

Uses **TCP port 21** for command **control** and **TCP port 20** for active mode **data** transfers.

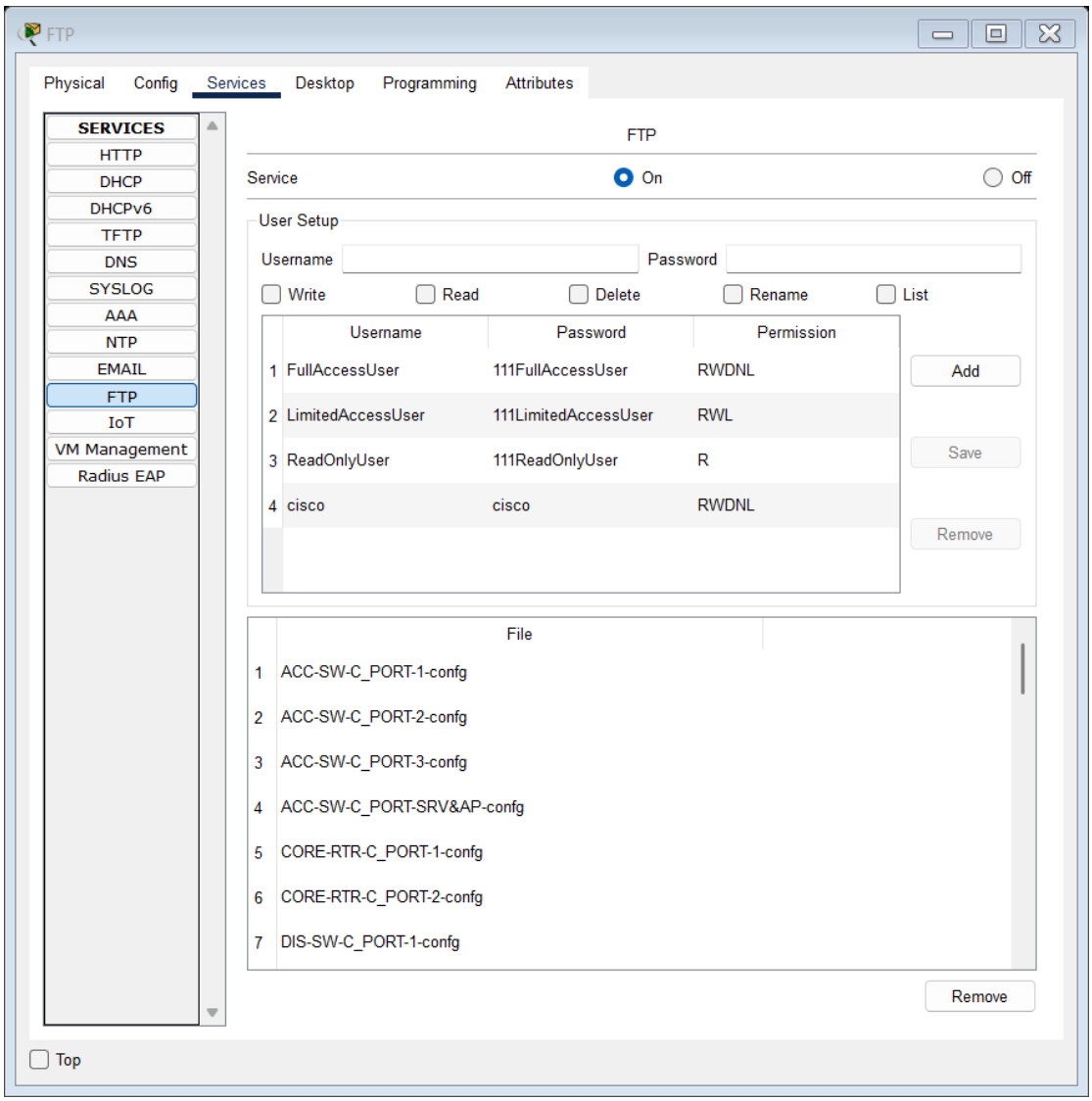
IOS Commands Alongside Their Descriptions:

Command	Description
ip ftp username *username*	Specifies the username for the authentication
ip ftp password *password*	Specifies the password for the authentication
copy *source_file* **ftp:***//ftp_server_ip_address/destination_file*	Copy the specified file to the FTP server.
Copy **ftp:***//ftp_server_ip_address/source_file destination_file*	Copy the specified from the FTP server to the device.

Sample execution of specified commands

CORE-RTR-C_PORT-1(config)#ip ftp username FullAccessUser
CORE-RTR-C_PORT-1(config)#ip ftp password 111FullAccessUser
CORE-RTR-C_PORT-1(config)#do copy startup-config ftp
Address or name of remote host []? ftp.mentoranexus.com
Destination filename [CORE-RTR-C_PORT-1-confg]?

Writing startup-config...Translating "ftp.mentoranexus.com"...domain server (10.60.111.100)
[OK - 4472 bytes]
4472 bytes copied in 0.021 secs (212000 bytes/sec)



Screenshot x.x — Codeport's FTP server file repository.

Trivial File Transfer Protocol (TFTP)

TFTP is a **connectionless**, lightweight **file transfer** protocol designed for bootstrapping network devices and distributing firmware or configurations. It omits authentication and encryption, relying on **predefined file directories**.

Employs **UDP port 69**.

IOS Commands Alongside Their Descriptions:

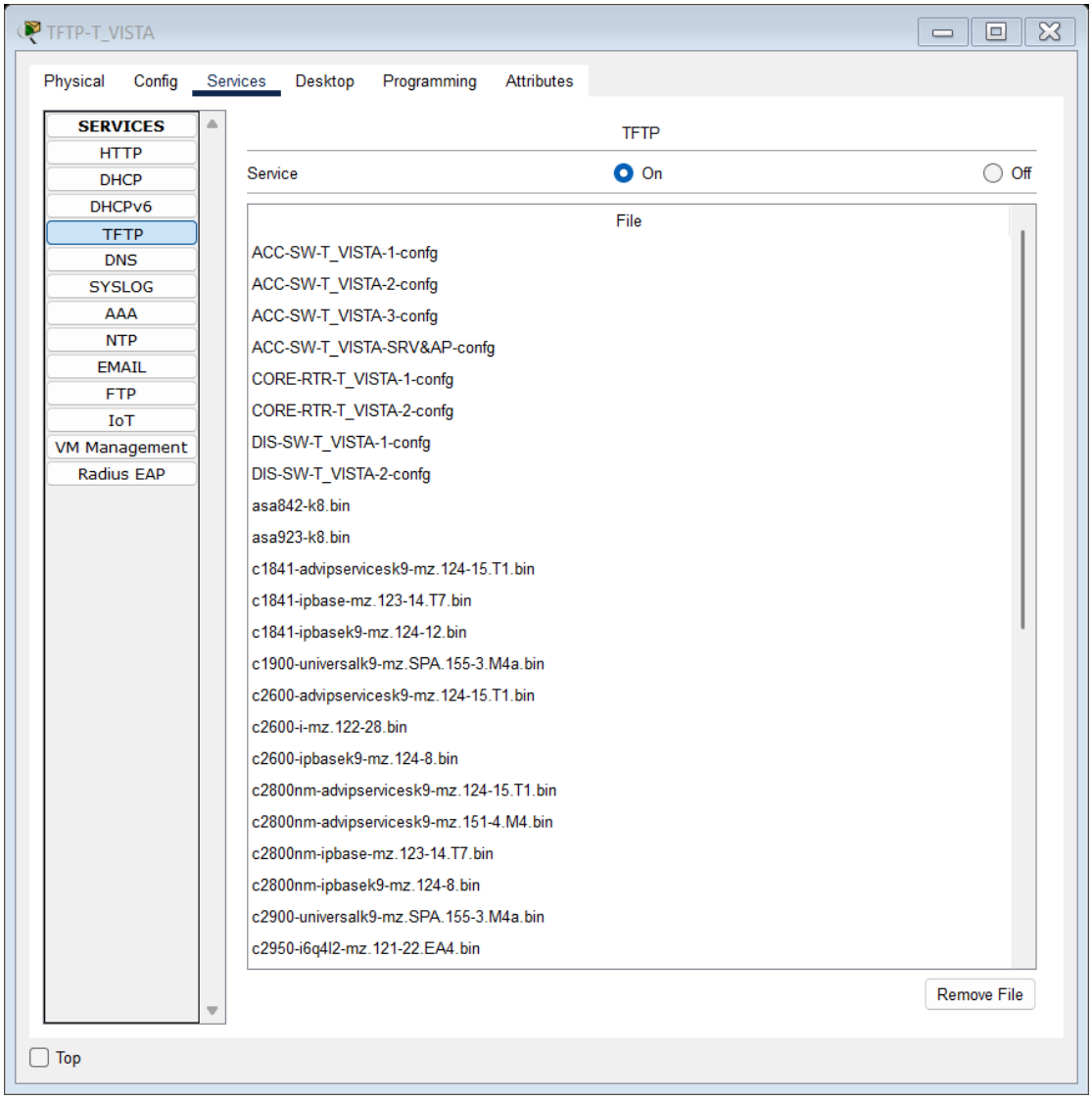
Command	Description
copy *source_file* **tftp:***//tftp_server_ip_address/destination_file*	Copy the specified file to the TFTP server.

Sample execution of specified commands

CORE-RTR-T_VISTA-1(config)#do copy startup-config tftp
Address or name of remote host []? tftp.techvista.mentoranexus.com
Destination filename [CORE-RTR-T_VISTA-1-confg]?

Writing startup-config...Translating "tftp.techvista.mentoranexus.com"...!!
[OK - 5837 bytes]

5837 bytes copied in 0.02 secs (291850 bytes/sec)



Screenshot x.x — TechVista's TFTP server file repository

Syslog Protocol

Syslog standardizes **event logging** across networked systems, structuring messages by **facility** (origin) and **severity** (importance). Messages can be forwarded to a remote **Syslog server** for **aggregation, analysis**, and **alerting**. Syslog messages have predefined value determining how severe they are. The lower this value, the more severe the message content, ranging from 0 to 7 with alternative terms (i.e., **debug** as an alternative for **7**).

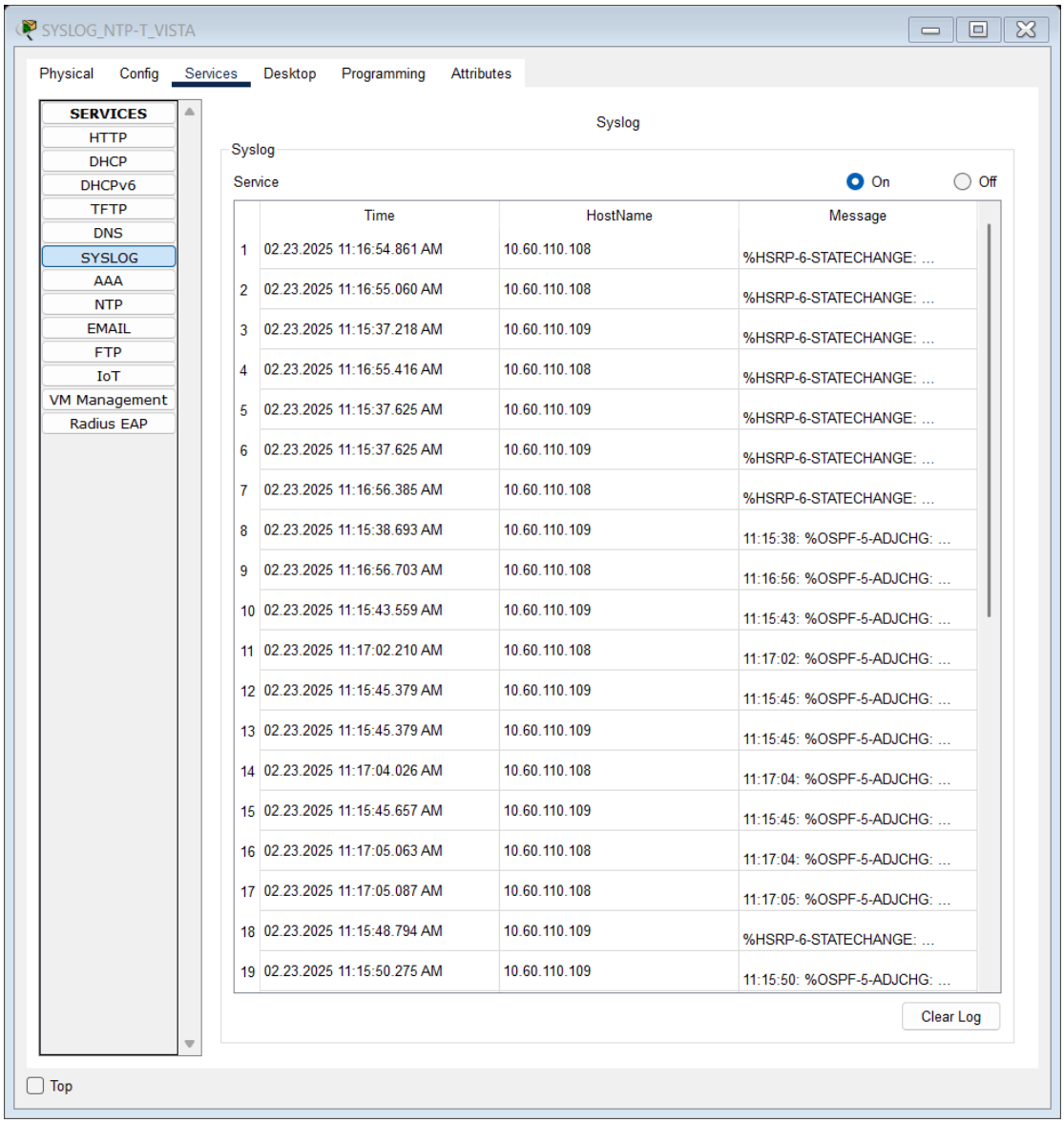
Operates primarily over **UDP port 514**.

IOS Commands Alongside Their Descriptions:

Command	**Description**
logging on	Enables transference of logging notifications to a remote Syslog server
logging *syslog_server_ip_address*	Specifies the Syslog server's IP address for storing the network device's syslog messages.
logging trap *severity_level*	The *severity_level* parameter defines which logging messages are to be sent to the syslog server with a default value of 7/debug.

Sample execution of specified commands

CORE-RTR-T_VISTA-1(config)#logging on
CORE-RTR-T_VISTA-1(config)#logging 10.60.110.99
CORE-RTR-T_VISTA-1(config)#logging trap debugging



Screenshot x.x — TechVista's Syslog server stores logging notifications.

Network Time Protocol (NTP)

NTP ensures precise **clock synchronization** across network nodes by employing a **hierarchical, stratum-based architecture**. It mitigates clock drift using the **Marzullo algorithm** and statistical filtering. NTP clients synchronize with a **reference clock** (stratum 1) through **intermediate servers** (stratum 2+), adjusting local time accordingly.

Uses **UDP port 123** for time synchronization.

On multi-layer switches and routers, the *ntp authentication-key* command **persists** after a reboot, whereas on Layer 2-only switches, it is **deleted** despite saving the configuration with *copy running-config startup-config*. This occurs because Layer 2 switches do not store encrypted authentication keys in the startup configuration for security reasons. As a solution, a SYSLOG server has been additionally configured as NTP server for Layer 2 switches without requiring authentication.

IOS Commands Alongside Their Descriptions:

Method	Command	Description
Authentication-Oriented NTP Synchronization	**ntp authenticate**	Enables NTP authentication, requiring valid keys for synchronization.
	ntp authentication-key *key* **md5** *password*	Defines an NTP authentication key using MD5 encryption.
	ntp server *ntp_server_ip_address* **key** *key_value*	Specifies an NTP server with authentication using a specified key .
	ntp update-calendar	Syncs the hardware clock (calendar) with the NTP time.
Authentication-Free NTP Synchronization	**ntp server** *ntp_server_ip_address*	Specifies an NTP server without requiring authentication.

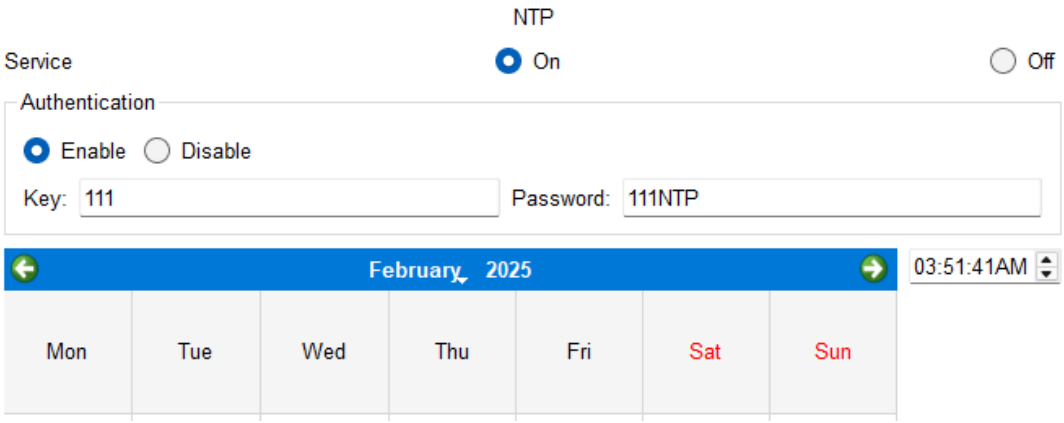
Sample execution of specified commands

Authentication-oriented implementation

CORE-RTR-T_VISTA-1(config)#ntp authentication-key 110 md5 110NTP
CORE-RTR-T_VISTA-1(config)#ntp authenticate
CORE-RTR-T_VISTA-1(config)#ntp trusted-key 110
CORE-RTR-T_VISTA-1(config)#ntp server 10.60.110.98 key 110
CORE-RTR-T_VISTA-1(config)#ntp update-calendar

Verifying using show commands

```
CORE-RTR-T_VISTA-1(config)#do sh ru | sec ntp
ntp authentication-key 110 md5 08701D1E272D35 7
ntp authenticate
ntp trusted-key 110
ntp server 10.60.110.98 key 110
ntp update-calendar
```



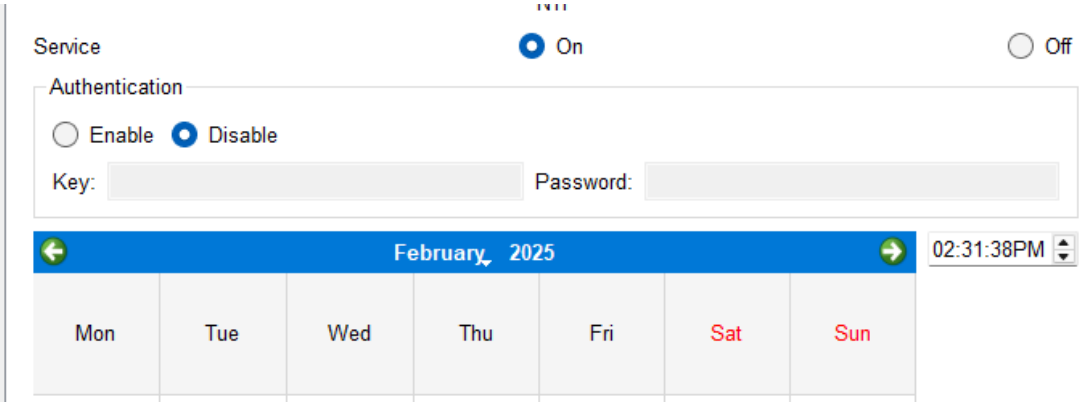
Screenshot x.x — TechVista's authentication-oriented NTP server.

Authentication-free implementation

DIS-SW-T_VISTA-1(config)#ntp server 10.60.110.99

Verifying using show commands

```
DIS-SW-T_VISTA-1(config)#do sh ru | sec ntp
ntp server 10.60.110.99
```

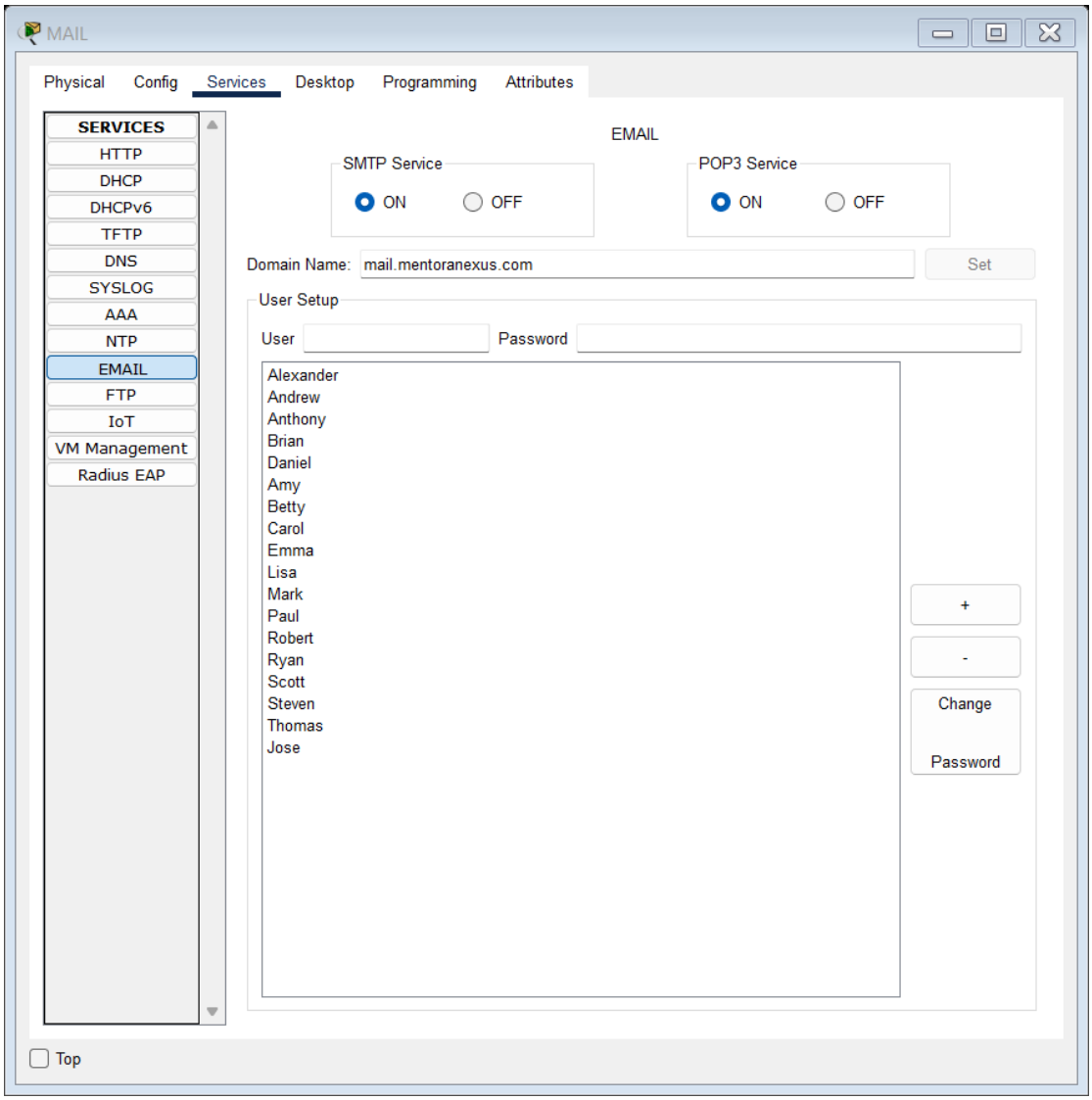


Screenshot x.x — TechVista's authentication-free NTP server.

Mail Protocols (SMTP, POP3, IMAP)

SMTP facilitates **mail transmission** between **mail servers**, while **POP3** and **IMAP** allow **client retrieval**. SMTP supports **STARTTLS** for encryption. IMAP provides **server-side** message management and concurrent multi-client access, whereas POP3 downloads messages **locally** and removes them from the server.

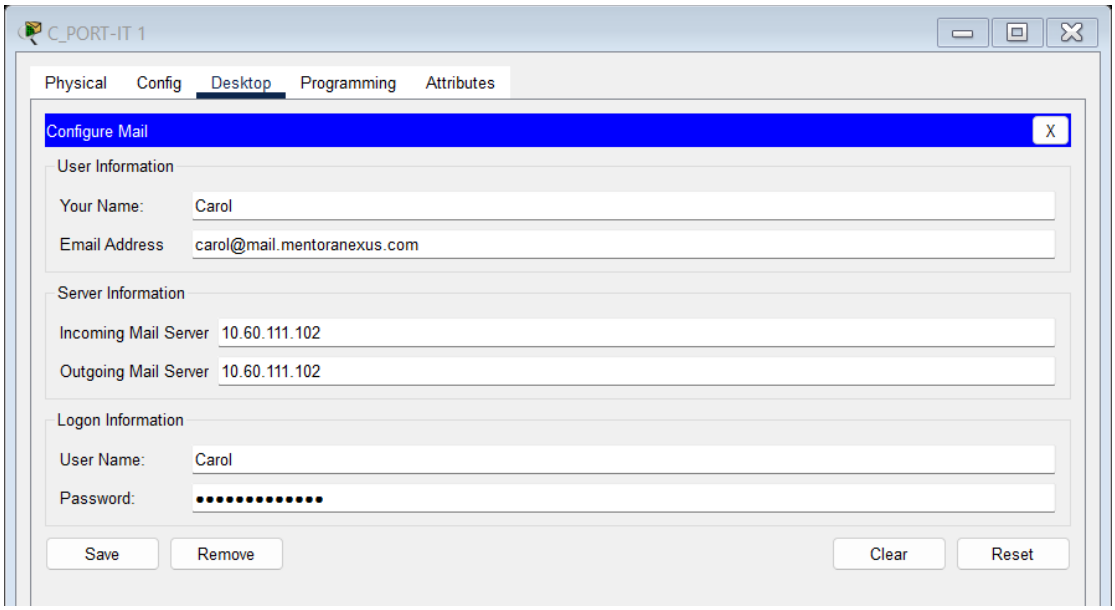
- SMTP: **TCP port 25** (relay), **587** (submission), **465** (TLS encryption).
- POP3: **TCP port 110** (unencrypted), **995** (SSL/TLS secure).
- IMAP: **TCP port 143** (unencrypted), **993** (SSL/TLS secure).



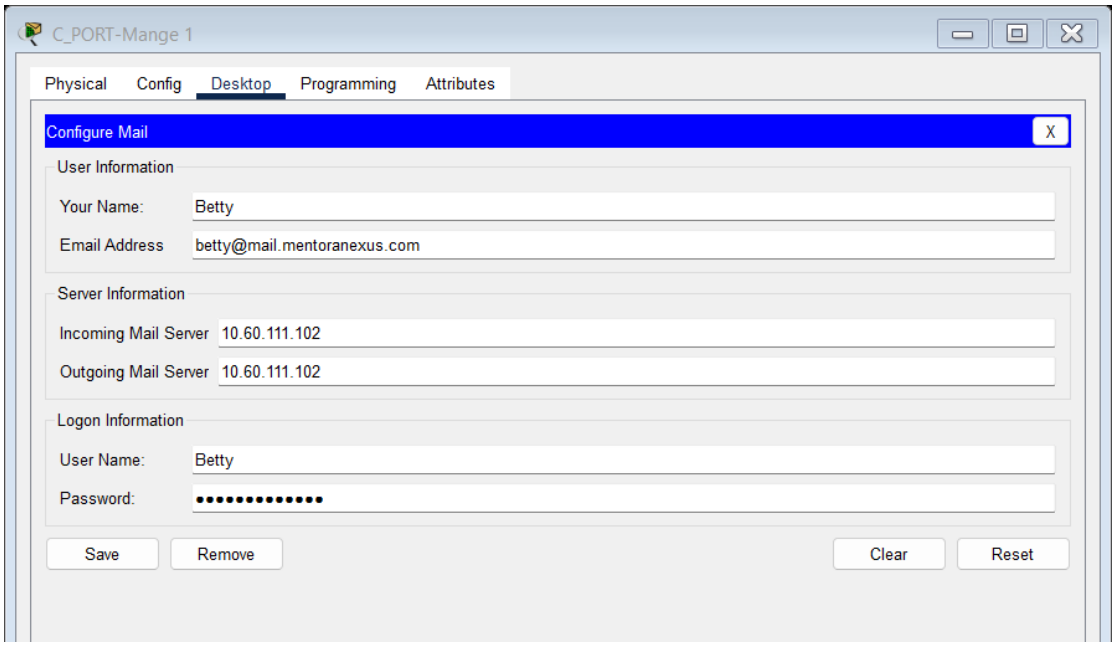
Screenshot x.x — Codeport's MAIL server configuration instance.

Illustration of Mail Exchange Between Two Employees

Configuring Email Clients on Employee Workstations.



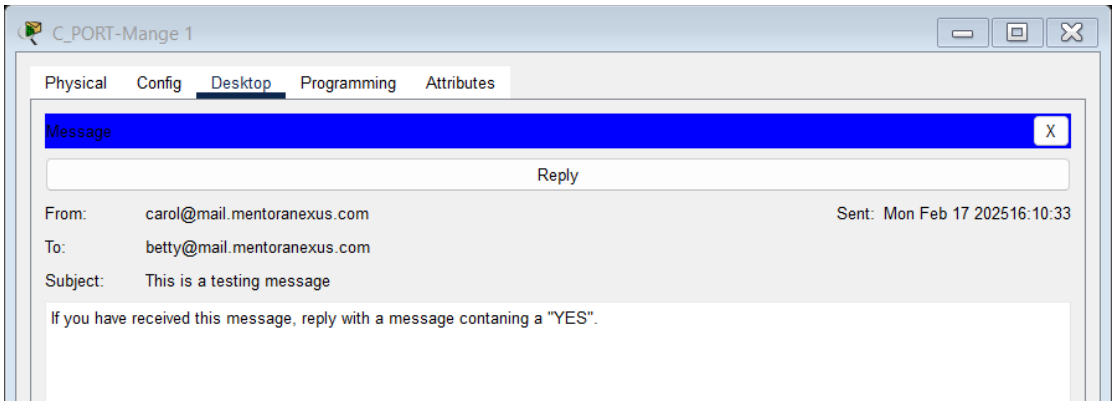
Screenshot x.x — Codeport PC1 mail configuration.



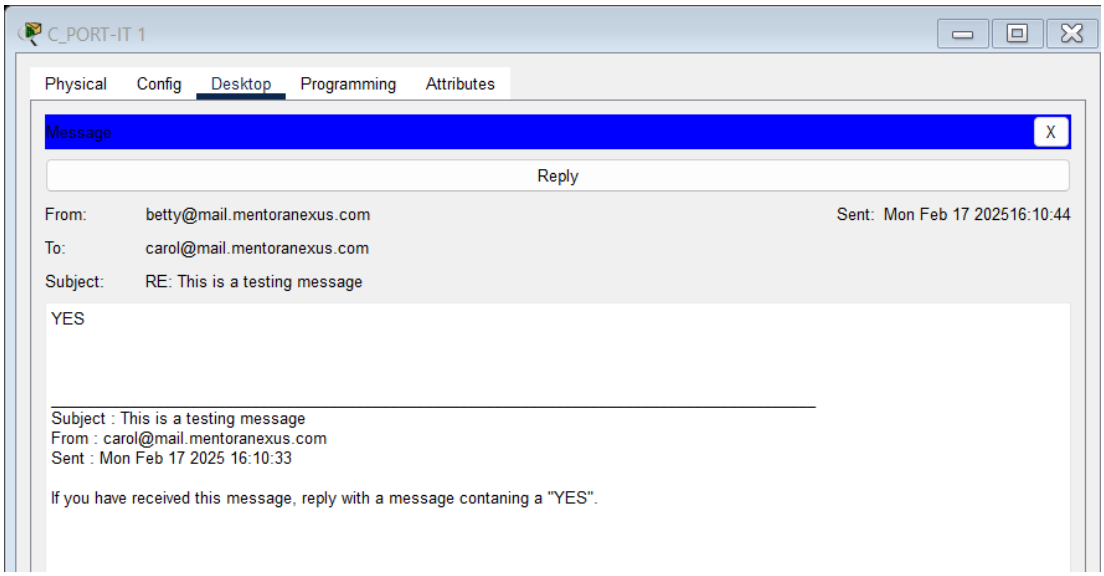
Screenshot x.x — Codeport PC2 mail configuration.

Testing Mail messages exchange functionality

1. **Transmission Initiation –** PC1 (Carol) generates and transmits a test packet.
2. **Reception and Response –** PC2 (Betty) receives the packet, processes it, and transmits a correspondence response.



3. **Acknowledgement –** PC1 successfully receives and validates the response from PC2, confirming bidirectional communication**.**



Authentication, Authorization, & Accounting (AAA)

AAA enforces **security policies** by **authenticating** users, **authorizing** access levels, and **tracking** network activity. It integrates with **RADIUS** (connectionless, UDP-based) and **TACACS+** (connection-oriented, TCP-based) protocols. RADIUS is preferred for network access authentication, whereas TACACS+ is used for device management and command authorization.

- RADIUS: **UDP ports 1812** (authentication) and **1813** (accounting).
- TACACS+: **TCP port 49**.

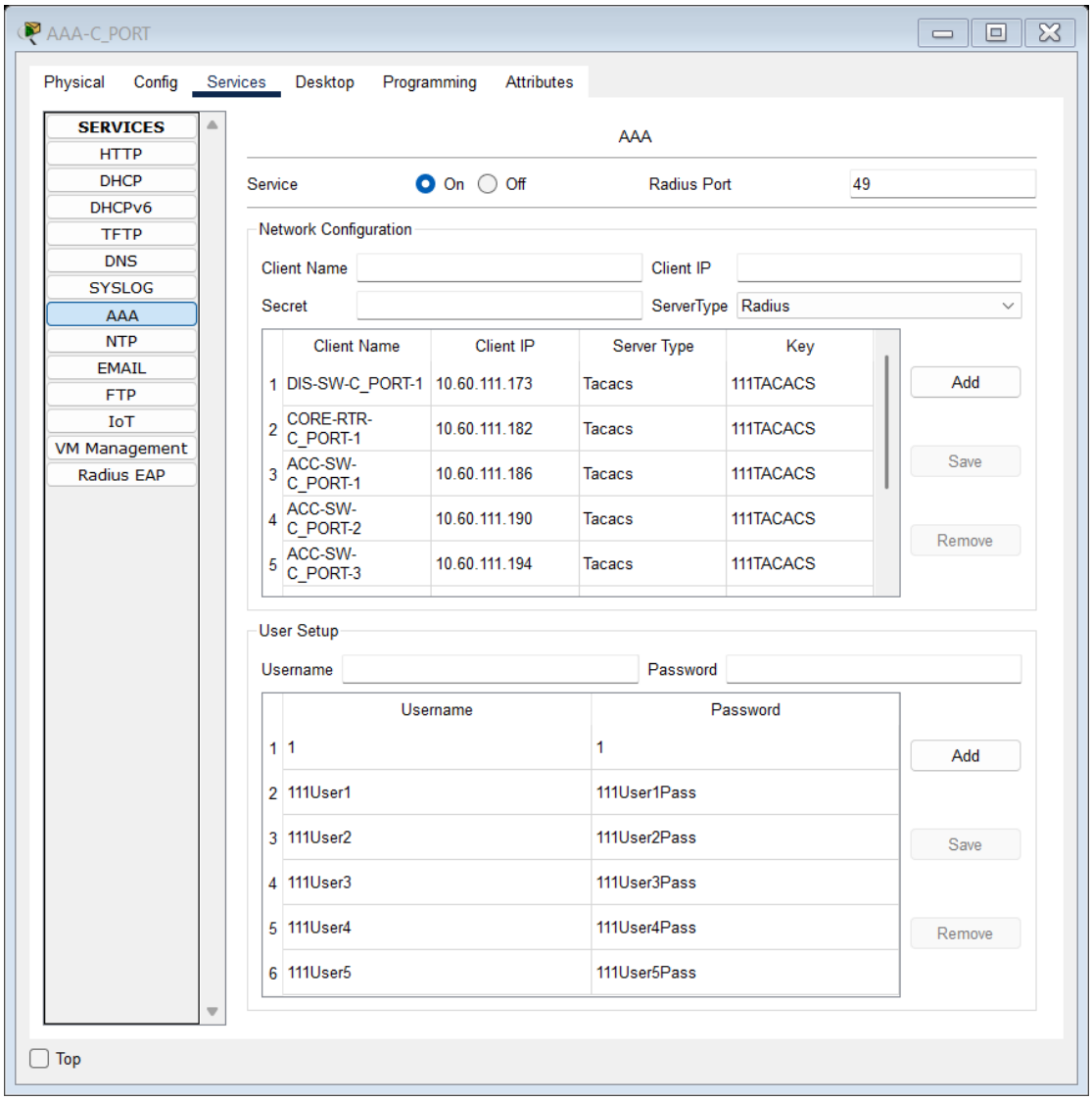
Configuring Radius/Tacacs authentication on PT-empty switches is not feasible. Instead, I have configured local authentication on those switches.

IOS Commands Alongside Their Descriptions:

Command	Description
aaa new-model	Enables the AAA (Authentication, Authorization, and Accounting) feature
aaa authentication login default group tacacs+ local	Configures login authentication using TACACS+, with local authentication as a fallback.
aaa authorization exec default group tacacs+ local	Enables command authorization via TACACS+, with local as a backup
aaa accounting exec default start-stop group tacacs+	Enables session accounting, logging start and stop events via TACACS+.
username admin privilege *level* **secret** *password*	Creates a user with a specified privilege level and encrypted password
tacacs-server host *tacacs_server_ip_address*	Defines the TACACS+ server's IP address for authentication.
tacacs-server key *key_value*	Sets the shared encryption key for TACACS+ communication
login authentication default	Applies the default AAA authentication method for login access on either VTY or Console connection or both.

Sample execution of specified commands

CORE-RTR-C_PORT-1(config)#aaa new-model
CORE-RTR-C_PORT-1(config)#aaa authentication login default group tacacs+ local
CORE-RTR-C_PORT-1(config)#aaa authorization exec default group tacacs+ local
CORE-RTR-C_PORT-1(config)#aaa accounting exec default start-stop group tacacs+
CORE-RTR-C_PORT-1(config)#username admin privilege 15 secret 5 ADMIN
CORE-RTR-C_PORT-1(config)#tacacs-server host 10.60.111.97
CORE-RTR-C_PORT-1(config)#tacacs-server key 111TACACS
CORE-RTR-C_PORT-1(config)#line vty 0 4
CORE-RTR-C_PORT-1(config-line)#login authentication default



Screenshot x.x — Codeport's AAA server configuration instance.

Dynamic Host Configuration Protocol (DHCP)

DHCP **dynamically allocates** IP addresses, subnet masks, default gateways, and DNS settings to clients. In a **router-based role**, it assigns addresses within a defined pool. As a **dedicated server**, it supports lease durations, reservations, and scope policies. DHCP relies on the **DORA** (Discovery, Offer, Request, Acknowledgment) process.

Uses **UDP port 67** (server) and **68** (client).

IOS Commands Alongside Their Descriptions

Command	Description
ip dhcp excluded-address *ip_address*	Excludes specific IP addresses from being assigned by the DHCP server.
ip dhcp pool vlan*VLAN_Number*	Creates a DHCP pool for a specific VLAN and enters DHCP configuration mode
network *subnet_address subnet_mask*	Defines the subnet and subnet mask for the DHCP pool.
default-router *default_gateway_ip_address*	Assigns the default gateway for DHCP clients.
dns-server *dns_server_ip_address*	Specifies the DNS server IP address for DHCP clients.
Ip helper-address *dhcp_server_ip_address*	Specifies the configured device to act as a DHCP relay agent

Sample execution of specified commands

Internal DHCP configuration

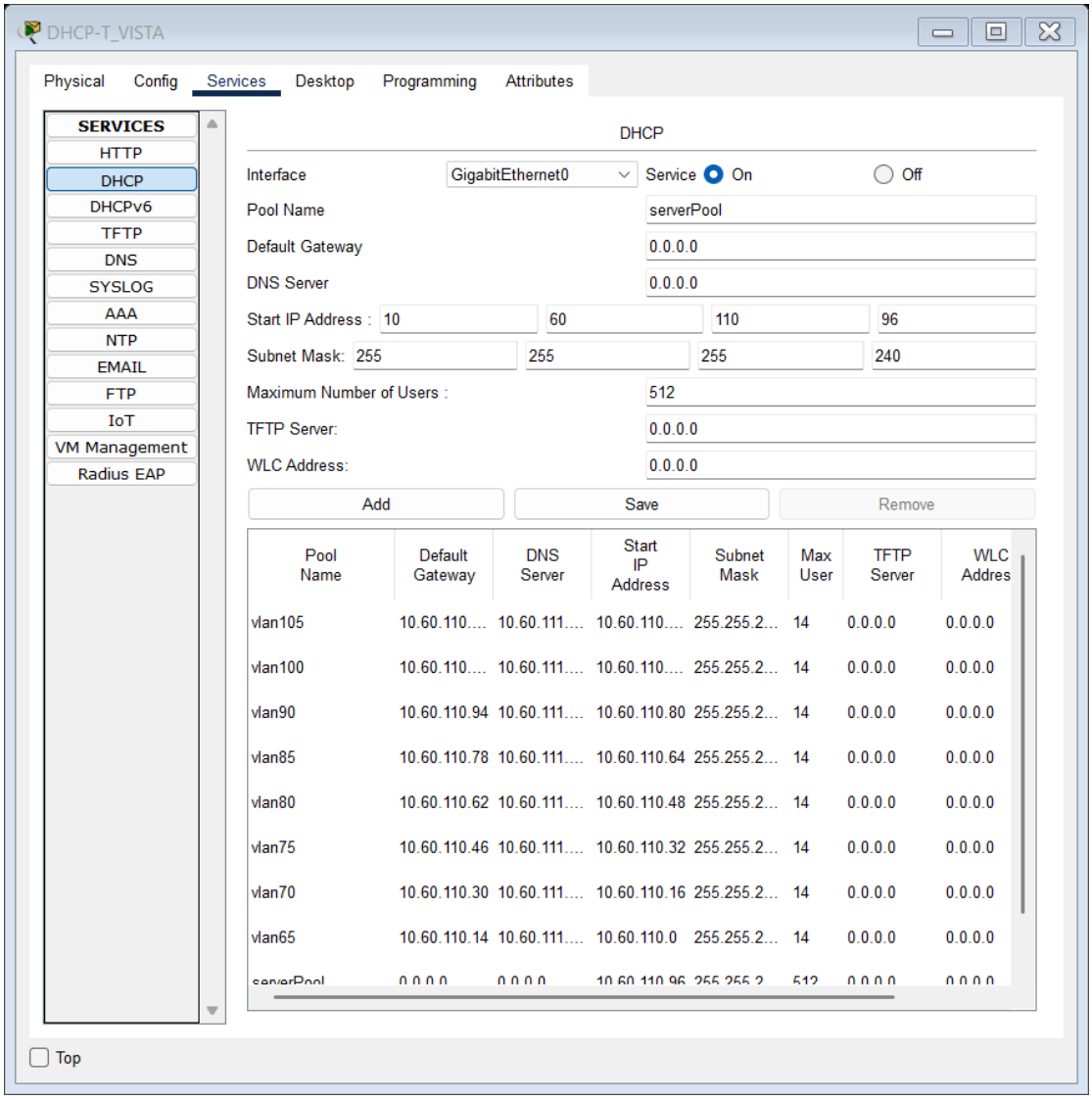
ACC-SW-C_PORT-3(config)#ip dhcp excluded-address 10.60.111.14
ACC-SW-C_PORT-3(config)#ip dhcp excluded-address 10.60.111.30
ACC-SW-C_PORT-3(config)#ip dhcp pool vlan110
ACC-SW-C_PORT-3(dhcp-config)# network 10.60.111.0 255.255.255.240
ACC-SW-C_PORT-3(dhcp-config)# default-router 10.60.111.14
ACC-SW-C_PORT-3(dhcp-config)# dns-server 10.60.111.100
ACC-SW-C_PORT-3(dhcp-config)#ip dhcp pool vlan115
ACC-SW-C_PORT-3(dhcp-config)# network 10.60.111.16 255.255.255.240
ACC-SW-C_PORT-3(dhcp-config)# default-router 10.60.111.30
ACC-SW-C_PORT-3(dhcp-config)# dns-server 10.60.111.100

```
ACC-SW-C_PORT-1(config)#do sh ru | sec dhcp
ip dhcp excluded-address 10.60.111.78
ip dhcp excluded-address 10.60.111.94
ip dhcp pool vlan130
 network 10.60.111.64 255.255.255.240
 default-router 10.60.111.78
 dns-server 10.60.111.100
ip dhcp pool vlan135
 network 10.60.111.80 255.255.255.240
 default-router 10.60.111.94
 dns-server 10.60.111.100
```

Example External DHCP configuration for VLAN 65

CORE-RTR-T_VISTA-1(config)#interface GigabitEthernet0/0.65
CORE-RTR-T_VISTA-1(config-subif)#ip helper-address 10.60.110.100

External DHCP configuration



Screenshot x.x — TechVista's external DHCP server configuration instance.

Routing Protocols

Open Shortest Path First (OSPF)

OSPF is an **intra-autonomous system, link-state routing protocol** that constructs a **complete network topology** using Link-State Advertisements (**LSAs**). It employs the **Dijkstra SPF algorithm** to calculate the shortest path. OSPF operates in hierarchical areas, reducing routing overhead. It supports equal-cost multipath (**ECMP**) and fast convergence.

Uses **IP protocol 89** (non-TCP/UDP).

Administrative Distance (**AD**): **110**.

IOS Commands Alongside Their Descriptions:

Command	Description
router ospf *process_id*	Enables OSPF, assigns a process ID, and enters OSPF configuration mode
router-id *id_value*	Manually sets the OSPF router ID.
low-adjacency-changes	Minimizes OSPF adjacency flaps by reducing unnecessary changes.
network *subnet_address subnet_mask* **area** *area_number*	Assigns a network to an OSPF area.
default-information-originate	Advertises a default route to OSPF neighbors.
passive interface *interface_name*	Prevents OSPF from sending hello packets on a specific interface while still advertising the network.
show ip ospf neighbor	Displays OSPF neighbors and their states.
show ip ospf database	Displays OSPF LSAs and the link-state database.
show ip ospf interface	Displays OSPF interface details, including cost, hello/dead timers, and adjacency status.

Sample execution of specified commands

DIS-SW-C_PORT-1(config)#router ospf 1
DIS-SW-C_PORT-1(config-router)#router-id 3.3.3.3
DIS-SW-C_PORT-1(config-router)#log-adjacency-changes
DIS-SW-C_PORT-1(config-router)#network 10.60.111.180 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.176 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.160 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.164 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.168 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.172 0.0.0.3 area 0
DIS-SW-C_PORT-1(config-router)#network 10.60.111.133 0.0.0.0 area 0

```
DIS-SW-C_PORT-1(config)#do sh ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:33    10.60.111.182   GigabitEthernet1/0/5
4.4.4.4           1   FULL/DR         00:00:33    10.60.111.178   Port-channel1
7.7.7.7           1   FULL/DR         00:00:34    10.60.111.166   GigabitEthernet1/0/2
6.6.6.6           1   FULL/DR         00:00:33    10.60.111.162   GigabitEthernet1/0/1
8.8.8.8           1   FULL/DR         00:00:33    10.60.111.170   GigabitEthernet1/0/3
5.5.5.5           1   FULL/DR         00:00:34    10.60.111.174   GigabitEthernet1/0/4
```

```
DIS-SW-C_PORT-1(config)#do sh ip ospf data
            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         685         0x80000004 0x00b170 2
3.3.3.3         3.3.3.3         680         0x8000000e 0x00728b 7
6.6.6.6         6.6.6.6         679         0x80000007 0x003f3e 4
4.4.4.4         4.4.4.4         679         0x8000000e 0x007199 7
2.2.2.2         2.2.2.2         679         0x80000004 0x0033bd 2
7.7.7.7         7.7.7.7         678         0x80000008 0x00f169 5
5.5.5.5         5.5.5.5         679         0x80000007 0x00f81c 4
8.8.8.8         8.8.8.8         679         0x80000008 0x0084fd 5

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.60.111.162   6.6.6.6         686         0x80000001 0x00471a
10.60.111.178   4.4.4.4         685         0x80000001 0x00bf9e
10.60.111.181   3.3.3.3         685         0x80000001 0x00b938
10.60.111.194   8.8.8.8         680         0x80000001 0x00d161
10.60.111.170   8.8.8.8         680         0x80000002 0x008cb0
10.60.111.166   7.7.7.7         680         0x80000001 0x008454
10.60.111.201   4.4.4.4         680         0x80000002 0x008fa8
10.60.111.174   5.5.5.5         680         0x80000002 0x00c87e
10.60.111.198   5.5.5.5         681         0x80000001 0x00d35a
10.60.111.186   6.6.6.6         679         0x80000002 0x00390e
10.60.111.190   7.7.7.7         678         0x80000002 0x00ff29

                Type-5 AS External Link States
Link ID         ADV Router      Age         Seq#       Checksum Tag
0.0.0.0         1.1.1.1         725         0x80000001 0x00fecf 1
0.0.0.0         2.2.2.2         724         0x80000001 0x00e0e9 1
```

Enhanced Interior Gateway Routing Protocol (EIGRP - Cisco Proprietary)

EIGRP is an **intra-autonomous system, advanced distance-vector** routing protocol **integrating link-state** characteristics. It employs the Diffusing Update Algorithm (**DUAL**) for **loop-free** route computation, supports unequal-cost multipath (**UCMP**) routing, and maintains a topology table for rapid convergence.

Uses **IP protocol 88**.

Administrative Distance (**AD**): **90** (internal routes), **170** (external routes).

IOS Commands Alongside Their Descriptions:

Command	Description

Have not implemented this routing protocol in my project. Therefore, is it acceptable to solely supply the fundamental principles of EIGRP, omitting the commands-descriptions table?

Border Gateway Protocol (BGP)

BGP is an **inter-autonomous system routing protocol** employing **path-vector** mechanics. It utilizes attributes such as **AS-PATH, NEXT-HOP, LOCAL_PREF**, and **MED** for path selection. **IBGP** (internal) operates within an AS, while **EBGP** (external) facilitates inter-AS routing.

Uses **TCP port 179.** Administrative Distance (**AD**): **20** (EBGP), **200** (IBGP).

IOS Commands Alongside Their Descriptions:

Command	Description
router bgp *ASN*	Enables BGP, assigns an Autonomous System Number (ASN) and enters BGP configuration mode
[no] bgp log-neighbor-changes	Logs BGP neighbor state changes; no disables logging
no synchronization	Disables the synchronization rule, allowing BGP to advertise routes without requiring IGP knowledge
neighbor *neighbor_ip_address* **remote-as** *neighbor_ASN*	Configures a BGP neighbor and assigns its remote ASN.
network *network_address* **mask** *network_mask*	Advertises a network into BGP using the specified subnet mask.
no auto-summary	Disables automatic summarization of classful networks in BGP.
show ip bgp summary	Displays a summary of BGP neighbors and statistics.
show ip bgp neighbors	Shows detailed information about BGP neighbor relationships.

Sample execution of specified command

ISP-RTR-1(config)#router bgp 10
ISP-RTR-1(config-router)# bgp log-neighbor-changes
ISP-RTR-1(config-router)# no synchronization
ISP-RTR-1(config-router)# neighbor 200.200.200.2 remote-as 20
ISP-RTR-1(config-router)# neighbor 200.200.200.3 remote-as 30
ISP-RTR-1(config-router)# neighbor 110.110.110.1 remote-as 110
ISP-RTR-1(config-router)# neighbor 110.110.110.2 remote-as 110
ISP-RTR-1(config-router)# network 200.200.200.0 mask 255.255.255.248
ISP-RTR-1(config-router)# network 110.110.110.0 mask 255.255.255.248

```
Router(config)#do sh ip bgp su
BGP router identifier 200.200.200.1, local AS number 10
BGP table version is 9, main routing table version 6
8 network entries using 1056 bytes of memory
8 path entries using 416 bytes of memory
6/4 BGP path/bestpath attribute entries using 920 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 2496 total bytes of memory
BGP activity 4/0 prefixes, 8/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
200.200.200.2   4    20      21      15        9    0    0 00:13:08        4
200.200.200.3   4    30      21      15        9    0    0 00:13:08        4
110.110.110.1   4   110       0       0        9    0    0 00:14:10        4
110.110.110.2   4   110       0       0        9    0    0 00:14:10        4
```

Layer 3 Protocols

Hot Standby Router Protocol (HSRP - Cisco Proprietary)

HSRP establishes a **virtual gateway** by electing an **active** and **standby** router, ensuring high availability through **priority-based failover**. **Preemption** and tracking mechanisms adjust roles dynamically.

Operates over **UDP port 1985**.

IOS Commands Alongside Their Descriptions:

Command	Description
standby *group_num* **ip** *virtual_ip_address*	Configures the virtual IP address for the HSRP group.
standby *group_num* **priority** *priority_value*	Sets the router's HSRP priority (higher value = preferred active router).
standby *group_num* **preempt**	Enables preemption, allowing a higher-priority router to take over the active role.
show standby	Displays HSRP status, including active/standby roles and timers.

Sample execution of specified commands

R1 – active for VLAN 65

CORE-RTR-T_VISTA-1(config)#interface GigabitEthernet0/0.65
CORE-RTR-T_VISTA-1(config-subif)#encapsulation dot1Q 65
CORE-RTR-T_VISTA-1(config-subif)#ip address 10.60.110.12 255.255.255.240
CORE-RTR-T_VISTA-1(config-subif)#ip helper-address 10.60.110.100
CORE-RTR-T_VISTA-1(config-subif)#standby 65 ip 10.60.110.14
CORE-RTR-T_VISTA-1(config-subif)#standby 65 priority 110
CORE-RTR-T_VISTA-1(config-subif)#standby 65 preempt

```
CORE-RTR-T_VISTA-1(config)#do sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         65   110 P Active   local           10.60.110.13    10.60.110.14
Gig         70   110 P Active   local           10.60.110.29    10.60.110.30
Gig         75   110 P Active   local           10.60.110.45    10.60.110.46
Gig         80   110 P Active   local           10.60.110.61    10.60.110.62
Gig         85   100 P Standby  10.60.110.76    local           10.60.110.78
Gig         90   100   Standby  10.60.110.92    local           10.60.110.94
Gig         95   100   Standby  10.60.110.108   local           10.60.110.110
Gig         100  100   Standby  10.60.110.124   local           10.60.110.126
Gig         105  100 P Standby  10.60.110.140   local           10.60.110.142
```

R2 – standby for VLAN 65

CORE-RTR-T_VISTA-1(config)#interface GigabitEthernet0/0.65
CORE-RTR-T_VISTA-1(config-subif)#encapsulation dot1Q 65
CORE-RTR-T_VISTA-1(config-subif)#ip address 10.60.110.13 255.255.255.240
CORE-RTR-T_VISTA-1(config-subif)#ip helper-address 10.60.110.100
CORE-RTR-T_VISTA-1(config-subif)#standby 65 ip 10.60.110.14

```
CORE-RTR-T_VISTA-2(config)#do sh standby bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig         65   100   Standby  10.60.110.12    local           10.60.110.14
Gig         70   100   Standby  10.60.110.28    local           10.60.110.30
Gig         75   100   Standby  10.60.110.44    local           10.60.110.46
Gig         80   100   Standby  10.60.110.60    local           10.60.110.62
Gig         85   110 P Active   local           10.60.110.77    10.60.110.78
Gig         90   110 P Active   local           10.60.110.93    10.60.110.94
Gig         95   110 P Active   local           10.60.110.109   10.60.110.110
Gig         100  110 P Active   local           10.60.110.125   10.60.110.126
Gig         105  110 P Active   local           10.60.110.141   10.60.110.142
```

IPsec Virtual Private Network (IPsec VPN)

IPsec **secures** IP communications via Encapsulating Security Payload (**ESP**) for **encryption** and Authentication Header (**AH**) for **integrity** verification. **IKE** (Internet Key Exchange) negotiates security parameters, supporting **Main** and **Aggressive** modes for **Phase 1** key exchange.

Uses **UDP port 500** (IKE negotiation), **ESP** (IP protocol 50), **AH** (IP protocol 51).

IOS Commands Alongside Their Descriptions:

Generic Routing Encapsulation (GRE)

GRE **encapsulates** Layer 3 packets, enabling tunneling over incompatible networks. It lacks intrinsic encryption, necessitating **IPsec integration** for confidentiality. **GRE tunnels** establish **stateless, point-to-point links**.

Encapsulation occurs under **IP protocol 47**.

IOS Commands Alongside Their Descriptions:

Command	**Description**
interface Tunnel*Tunnel_ID*	Creates and enters a tunnel interface configuration mode
ip address *tunnel_ip_address tunnel_subnet_mask*	Assigns an IP address and subnet mask to the tunnel interface
tunnel source *interface_name*	Specifies the source interface for the tunnel.
tunnel destination *peer_ip_address*	Defines the remote peer's IP address as the tunnel endpoint.
show interfaces tunnel *Tunnel_ID*	Displays the status, IP address, MTU, and encapsulation type of the GRE tunnel.

Sample execution of specified commands

CORE-RTR-T_VISTA-1(config)#interface Tunnel11011101
CORE-RTR-T_VISTA-1(config-if)#ip address 192.168.1.1 255.255.255.252
CORE-RTR-T_VISTA-1(config-if)#tunnel source GigabitEthernet0/0/0
CORE-RTR-T_VISTA-1(config-if)#tunnel destination 111.111.111.1

```
CORE-RTR-T_VISTA-1(config)#do sh int tunnel 11011101
Tunnel11011101 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 110.110.110.1 (GigabitEthernet0/0/0), destination 111.111.111.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

EtherChannel (Cisco Proprietary)

EtherChannel **aggregates** multiple physical links into a **single logical interface**, increasing bandwidth and redundancy. It supports **static**, **PAgP** (Cisco proprietary), and **LACP** (IEEE 802.3ad) negotiation.

LACP utilizes multicast **MAC address 01-80-C2-00-00-02.**

Note: EtherChannel can also operates as a layer 2 protocol despite its present in this section.

IOS Commands Alongside Their Descriptions:

Command	Description
Interface Port-channel*ID*	Creates and enters a Port-Channel (EtherChannel) interface configuration mode.
channel-group *Port-channelID* **mode on**	Assigns an interface to a Port-Channel and forces static EtherChannel (no negotiation).
show etherchannel summary	Displays EtherChannel status and configuration.
show etherchannel port-channel	Provides details of the Port-Channel interface.

Sample execution of specified commands

DIS-SW-C_PORT-1(config)#interface Port-channel1
DIS-SW-C_PORT-1(config-if)#no switchport

*Feb 24, 04:46:00.4646: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

*Feb 24, 04:46:00.4646: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

DIS-SW-C_PORT-1(config-if)#ip address 10.60.111.177 255.255.255.252
DIS-SW-C_PORT-1(config-if)#interface GigabitEthernet1/0/23
DIS-SW-C_PORT-1(config-if)#no switchport
DIS-SW-C_PORT-1(config-if)#no ip address
DIS-SW-C_PORT-1(config-if)#channel-group 1 mode on
DIS-SW-C_PORT-1(config-if)#interface GigabitEthernet1/0/24
DIS-SW-C_PORT-1(config-if)#no switchport
DIS-SW-C_PORT-1(config-if)#no ip address
DIS-SW-C_PORT-1(config-if)#channel-group 1 mode on
DIS-SW-C_PORT-1(config-if)#

```
DIS-SW-C_PORT-1(config)#do sh etherchannel su
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Po1(RU)           -      Gig1/0/23(P) Gig1/0/24(P)
```

Layer 2 Protocols

VLAN Trunking Protocol (VTP - Cisco Proprietary)

VTP **synchronizes VLAN databases** across switches, reducing administrative overhead. It functions in **server**, **client**, and **transparent** modes, with version 3 supporting **MST** (Multiple Spanning Tree) integration. Uses multicast **MAC address 01-00-0C-CC-CC-CC** on VLAN 1.

IOS Commands Alongside Their Descriptions:

Command	Description
vtp mode (*transport / client / server***)**	Sets the VTP mode: **server** (can create, modify, and propagate VLANs), **client** (receives updates but cannot create VLANs), or **transparent** (forwards updates but does not participate in VTP).
vtp domain *domain_name*	Assigns the switch to a specific VTP domain for VLAN synchronization.
vtp password *pass*	Configures a password for VTP authentication, ensuring only authorized switches can exchange VLAN information.
vtp version *ver*	Specifies the VTP version (1, 2, or 3), affecting features and VLAN propagation.
[no] vtp pruning	Enables **VTP pruning**, which limits VLAN traffic to only switches that need it.
show vtp status	Displays VTP configuration details, including mode, domain, version, and VLAN statistics.
show vtp counters	Shows VTP message statistics, including advertisements sent, received, and errors.

Sample execution of specified commands

DIS-SW-T_VISTA-1(config)#vtp mode server
Setting device to VTP SERVER mode.
DIS-SW-T_VISTA-1(config)#vtp domain mentoranexus.com
Changing VTP domain name from . to mentoranexus.com
DIS-SW-T_VISTA-1(config)#vtp password vtp1234
Setting device VLAN database password to vtp1234
DIS-SW-T_VISTA-1(config)#vtp version 2

```
DIS-SW-T_VISTA-1(config)#do sh vtp st
VTP Version                     : 2
Configuration Revision          : 1188
Maximum VLANs supported locally : 255
Number of existing VLANs        : 14
VTP Operating Mode              : Server
VTP Domain Name                 : mentoranexus.com
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x21 0xB7 0xC9 0x6F 0x20 0x8F 0xA9 0xCB
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.60.110.133 on interface Vl105 (lowest numbered VLAN interface found)
```

```
DIS-SW-T_VISTA-1(config)#do sh vtp counters
VTP statistics:
Summary advertisements received    : 23
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 35
Subset advertisements transmitted  : 19
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
```

Rapid Spanning Tree Protocol (RSTP - IEEE 802.1w)

RSTP optimizes **spanning tree convergence** using **port roles** (**Root, Designated, Alternate, Backup**) and introduces proposal/agreement mechanisms. It improves upon **802.1D** by eliminating timers in favor of immediate state transitions.

Operates via Bridge Protocol Data Units (**BPDUs**) within IEEE **802.1D frames**.

IOS Commands Alongside Their Descriptions:

Command	Description
spanning-tree mode *(pvst / rapid-pvst)*	Selects PVST or Rapid PVST mode
spanning-tree vlan *vlan_id* **priority** *priority_value*	Sets the spanning-tree priority for a specific VLAN.
spanning-tree vlan *vlan_id* **root (***primary / secondary***)**	Configures the switch as the primary / secondary root bridge for a specific VLAN.
spanning-tree portfast	Enables PortFast on an interface, allowing it to transition to forwarding state immediately.
spanning-tree bpduguard enable	Enables BPDU Guard, disabling ports that receive BPDU packets.
show spanning-tree	Displays spanning-tree status and configuration details.

Sample execution of specified commands

ACC-SW-T_VISTA-1(config)#spanning-tree mode pvst
ACC-SW-T_VISTA-1(config)#spanning-tree vlan 65,70,75,80,85,90,95,100,105 priority 24576
ACC-SW-T_VISTA-1(config)#interface FastEthernet0/1
ACC-SW-T_VISTA-1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
ACC-SW-T_VISTA-1(config-if)#spanning-tree bpduguard enable

```
ACC-SW-T_VISTA-1(config)#do sh sp
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0000.0C43.48ED
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B008.B68B
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 4         128.25   P2p
Gi0/2            Desg FWD 4         128.26   P2p

VLAN0065
  Spanning tree enabled protocol ieee
  Root ID     Priority    24641
              Address     0000.0C43.48ED
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32833  (priority 32768 sys-id-ext 65)
              Address     00E0.B008.B68B
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/15           Desg FWD 19        128.15   P2p
Fa0/17           Desg FWD 19        128.17   P2p
Fa0/13           Desg FWD 19        128.13   P2p
Fa0/12           Desg FWD 19        128.12   P2p
Fa0/14           Desg FWD 19        128.14   P2p
Fa0/16           Desg FWD 19        128.16   P2p
Fa0/19           Desg FWD 19        128.19   P2p
Gi0/1            Root FWD 4         128.25   P2p
Fa0/18           Desg FWD 19        128.18   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Trunking (IEEE 802.1Q - Dot1Q)

802.1Q **encapsulates VLAN information** within Ethernet frames using a **4-byte tag**, ensuring VLAN segmentation over a single trunk link. It designates a **Native VLAN** for untagged traffic and supports **VLAN pruning** to optimize broadcast domains.

Encodes VLAN identifiers within Ethernet frames (no dedicated port).

IOS Commands Alongside Their Descriptions:

Command	Description
switchport mode trunk	Sets the port to trunk mode, enabling multiple VLANs to traverse the link.
switchport trunk encapsulation dot1q	Specifies 802.1Q as the trunking protocol.
switchport trunk allowed vlan *vlan_list*	Defines which VLANs are permitted to pass through the trunk.
switchport trunk native vlan *vlan_id*	Configures the VLAN ID that will be untagged on the trunk port (default is VLAN 1).
show *interface* **switchport**	Displays information about trunk ports, including allowed VLANs and encapsulation type.
show vlan brief	Lists all VLANs and their associated ports, helping to verify 802.1Q configurations.

```
ACC-SW-T_VISTA-1(config)#do sh vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
65   TVISTA_MGMT                       active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19
70   TVISTA_IT                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
75   ACADPUB                           active
80   TECHINN                           active
85   HR                                active
90   FIN                               active
95   TVISTA_SRV                        active
100  TVISTA_AP                         active
105  TVISTA_NETCONF                    active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
ACC-SW-T_VISTA-1(config)#do sh int fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 70 (TVISTA_IT)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Miscellaneous IOS Commands

Device Identification and Basic Configuration

hostname *hostname-entry* modifies the device's hostname.

```
Router(config)#hostname CORE-RTR-T_VISTA-1
CORE-RTR-T_VISTA-1(config)#
```

ip domain-name *domain-name-value* defines the device's domain name. Employed in DNS lookups and SSH.

```
CORE-RTR-T_VISTA-1(config)#ip domain-name montoranexus.techvista.com
CORE-RTR-T_VISTA-1(config)#do sh ru | i dom
ip domain-name montoranexus.techvista.com
```

ip default-gateway *gateway-ip* sets the default gateway IP address for the device.

```
ACC-SW-T_VISTA-1(config)#ip default-gateway 10.60.110.142
ACC-SW-T_VISTA-1(config)#do sh r | i default-g
ip default-gateway 10.60.110.142
```

Security, Authentication, and Line Connections

enable secret *secret-password* defines a secret password to be hashed for protecting privileged EXEC mode.

```
ACC-SW-T_VISTA-1(config)#enable secret 110SECRET
ACC-SW-T_VISTA-1(config)#do sh r | i enable s
enable secret 5 $1$mERr$Vl75q4kDIboc0VhRxfxvt1
```

enable password plaintext-password defines a plaintext password to protect privileged EXEC mode.

```
ACC-SW-T_VISTA-1(config)#enable password 110PASSWORD
ACC-SW-T_VISTA-1(config)#do sh r | i enable p
enable password 110PASSWORD
```

service password-encryption encrypts plaintext passwords within the device's configuration file.

```
ACC-SW-T_VISTA-1(config)#enable password 110PASSWORD
ACC-SW-T_VISTA-1(config)#do sh r | i enable p
enable password 110PASSWORD
ACC-SW-T_VISTA-1(config)#service password-encryption
ACC-SW-T_VISTA-1(config)#do sh r | i enable p
enable password 7 08701D1E3938362425243E20
```

ip ssh version *<1|2>* specifies the SSH protocol version used by the device.

```
ACC-SW-T_VISTA-1(config)#ip ssh version 2
ACC-SW-T_VISTA-1(config)#do sh r | i ssh v
ip ssh version 2
```

crypto key generate rsa *[modulus <512–2048>]* generates RSA key pairs to enable SSH secure connections.

```
ACC-SW-T_VISTA-1(config)#crypto key generate rsa
% You already have RSA keys defined named ACC-SW-T_VISTA-1.montoranexus.techvista.com .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: ACC-SW-T_VISTA-1.montoranexus.techvista.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

login *[local]* enables password checking; optionally specifies local username/password authentication.

```
ACC-SW-T_VISTA-1(config)#line vty 0 4
ACC-SW-T_VISTA-1(config-line)#password Pa1ss2wo3rd4
ACC-SW-T_VISTA-1(config-line)#login
```

line vty *<0-4|0-15>* enters VTY line configuration for remote access sessions (SSH/Telnet).

transport input *<ssh | telnet | all | none>* specifies permitted protocols (SSH, Telnet, or both) for VTY line access.

exec-timeout *<minutes> [seconds]* sets idle timeout duration for console or VTY sessions.

```
ACC-SW-T_VISTA-1(config)#line vty 0 4
ACC-SW-T_VISTA-1(config-line)#transport input ssh
ACC-SW-T_VISTA-1(config-line)#exec-timeout 30 0
ACC-SW-T_VISTA-1(config-line)#do sh r | s vty
line vty 0 4
 exec-timeout 30 0
 password 7 08114D1F1A0A57001D581E007E
 logging synchronous
 login authentication default
 transport input ssh
```

ip arp inspection vlan *<vlan-range>* enables Dynamic ARP Inspection on specified VLAN(s) to prevent ARP spoofing.

```
ACC-SW-T_VISTA-1(config)#ip arp inspection vlan 65,70
ACC-SW-T_VISTA-1(config)#do sh r | s ip arp inspection v
ip arp inspection vlan 65,70
```

ip dhcp snooping vlan *<vlan-range>* enables DHCP snooping security feature on specified VLAN(s).

```
ACC-SW-T_VISTA-1(config)#ip dhcp snooping vlan 65,70
ACC-SW-T_VISTA-1(config)#do sh r | s ip dhcp snooping v
ip dhcp snooping vlan 65,70
```

interface *<type number> (e.g., GigabitEthernet0/1, FastEthernet0/0)* enters interface configuration mode for the specified interface.

ip arp inspection trust marks an interface as trusted for Dynamic ARP Inspection purposes.

ip dhcp snooping trust configures the interface as trusted for DHCP snooping (allows DHCP server replies).

```
ACC-SW-T_VISTA-1(config)#int g0/1
ACC-SW-T_VISTA-1(config-if)#ip dhcp snooping trust
ACC-SW-T_VISTA-1(config-if)#ip arp inspection trust
```

```
interface GigabitEthernet0/1
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
```

Logging and Monitoring

service timestamps log datetime msec adds date, time, and millisecond precision to log messages.

service timestamps debug datetime msec adds precise timestamps to debug messages for troubleshooting.

```
ACC-SW-T_VISTA-1(config)#service timestamps log datetime msec
ACC-SW-T_VISTA-1(config)#service timestamps debug datetime msec
```

line con 0 enters console line configuration mode for managing console port settings.

logging synchronous ensures log and debug output do not interrupt command-line entry.

```
ACC-SW-T_VISTA-1(config)#line con 0
ACC-SW-T_VISTA-1(config-line)#logging synchronous
ACC-SW-T_VISTA-1(config-line)#line vty 0 4
ACC-SW-T_VISTA-1(config-line)#logging synchronous
```

show running-config displays the active configuration currently running in memory.

show startup-config displays the configuration stored in NVRAM (startup configuration).

show interfaces *[type number]* provides detailed status and statistics for device interfaces.

show ip protocols displays active routing protocols and their configurations.

show vlan brief summarizes VLAN IDs, names, statuses, and assigned ports.

Banner and User Access

banner motd *<delimiter>* Your Message Here *<delimiter>* defines a Message-of-the-Day banner displayed upon device login.

```
ACC-SW-T_VISTA-1(config)#banner motd ~
Enter TEXT message.  End with the character '~'.
Unauthorized access my lead to undesired consequences!
~

Press RETURN to get started.
```

```
Unauthorized access my lead to undesired consequences!
```

VLAN and Interface Management

no shutdown activates (turns on) the specified interface or VLAN.

vlan *<vlan-id>* creates or enters configuration mode for a specific VLAN.

name *<vlan-name>* assigns a descriptive name to a VLAN.

```
ACC-SW-T_VISTA-1(config)#int g0/1
ACC-SW-T_VISTA-1(config-if)#no shutdown

ACC-SW-T_VISTA-1(config-if)#
*Feb 17, 14:37:40.3737: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
*Feb 17, 14:37:40.3737: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
ACC-SW-T_VISTA-1(config-if)#ex
ACC-SW-T_VISTA-1(config)#vlan 10
ACC-SW-T_VISTA-1(config-vlan)#name IT
```

Routing and ACL Management

ip route *<destination-network> <subnet-mask> <next-hop-ip | exit-interface>* defines a static route to a specified network via next-hop IP or exit interface.

```
CORE-RTR-T_VISTA-1(config)#ip route 0.0.0.0 0.0.0.0 110.110.110.3
CORE-RTR-T_VISTA-1(config)#ip route 10.60.111.0 255.255.255.0 192.168.1.2
CORE-RTR-T_VISTA-1(config)#ip route 10.60.112.0 255.255.255.0 192.168.1.6
CORE-RTR-T_VISTA-1(config)#do sh ip ro sta
     10.0.0.0/8 is variably subnetted, 20 subnets, 3 masks
S       10.60.111.0/24 [1/0] via 192.168.1.2
S       10.60.112.0/24 [1/0] via 192.168.1.6
S*   0.0.0.0/0 [1/0] via 110.110.110.3
```

ip access-list *<standard | extended> <name | number>* creates or modifies an IP access control list to filter network traffic.

```
CORE-RTR-T_VISTA-1(config-std-nacl)#ip access-list standard VTY_ACCESS
CORE-RTR-T_VISTA-1(config-std-nacl)# permit 10.60.110.0 0.0.0.15
CORE-RTR-T_VISTA-1(config-std-nacl)# permit 10.60.110.16 0.0.0.15
CORE-RTR-T_VISTA-1(config-std-nacl)# deny any
CORE-RTR-T_VISTA-1(config-std-nacl)# remark Access via VTY is strictly restricted to the
Management and IT departments
CORE-RTR-T_VISTA-1(config-std-nacl)#do sh access-list
Standard IP access list VTY_ACCESS
    10 permit 10.60.110.0 0.0.0.15
    20 permit 10.60.110.16 0.0.0.15
    30 deny any
```

Maintenance and Operational Commands

write *[memory] (or equivalently* copy running-config startup-config*)* saves current running configuration to NVRAM.

reload restarts the device (reboots IOS).

clear *<parameter>* (e.g., clear counters, clear ip route, clear arp-cache) clears specified operational or statistical information.

no *<command-to-negate>* removes or negates a previously applied command.

no cdp run disables Cisco Discovery Protocol globally on the device.